View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by DigitalCommons@Kennesaw State University

Kennesaw State University
DigitalCommons@Kennesaw State University

KSU Proceedings on Cybersecurity Education, Research and Practice

2019 KSU Conference on Cybersecurity Education, Research and Practice

Oct 12th, 11:30 AM - 11:55 AM

IOT: Challenges in Information Security Training

Lech J. Janczewski
The University of Auckland, lech@auckland.ac.nz

Gerard Ward
The University of Auckland, gerard.ward@auckland.ac.nz

Follow this and additional works at: https://digitalcommons.kennesaw.edu/ccerp

Part of the Information Security Commons, Management Information Systems Commons, and the Technology and Innovation Commons

Janczewski, Lech J. and Ward, Gerard, "IOT: Challenges in Information Security Training" (2019). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 3.
https://digitalcommons.kennesaw.edu/ccerp/2019/education/3

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Abstract
Both consumers and businesses are rapidly adopting IoT premised on convenience and control. Industry and academic literature talk about billions of embedded IoT devices being implemented with use-cases ranging from smart speakers in the home, to autonomous trucks, and trains operating in remote industrial sites. Historically information systems supporting these disparate use-cases have been categorised as Information Technology (IT) or Operational Technology (OT), but IoT represents a fusion between these traditionally distinct information security models.

This paper presents a review of IEEE and Elsevier peer reviewed papers that identifies the direction in IoT education and training around information security. It concludes that the education/training still is largely distinct and is not addressing the needs of this hybrid IT and OT model. IoT is complex as it melds embedded systems and software in support of interaction with physical systems. While literature contains implementation specific research, papers that address appropriate methodologies and content around secure design are piecemeal in nature.

We conclude that in the rush to find implementation specific strategies the overarching strategy around education and training of secure IoT design is not being adequately addressed. Consequently, we propose a novel approach to how IoT education training can better incorporate the topic of secure design at a foundational level.

Location
KSU Center Rm 460

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Comments
Key words

IoT, IIoT, Information Technology, Operational Technology, Security, Education, Training, Secure Design

This event is available at DigitalCommons@Kennesaw State University: https://digitalcommons.kennesaw.edu/ccerp/2019/education/3

INTRODUCTION

This paper summarises IoT development trends. It presents the results of research aimed at identifying the direction of IoT education and training, principally the initiatives directed at addressing information security. A review of IEEE and Elsevier peer reviewed papers was conducted to establish the trends in IoT development, and the extent to which they are, as well as should be addressed by the education sector.

TRENDS IN DEVELOPMENT OF IoT-BASE SYSTEM

IoT Security

The Internet of Things (IoT) is tipped to revolutionise the way we engage with one another, the quality of services we receive, and how we interact with our environment. While these IoT connections will be supported by a technical platform, the functional benefits are promoted based on IoT devices requiring minimal configuration, delivering high system availability, and providing a speed of computation to deliver the desired user experience.

IoT continues the progress in electronics and software of the last 50 years that has resulted in a dramatic increase in the capability of digital devices. For consumers the uptake of IoT is premised on convenience; responsiveness; and greater control delivering efficiencies like the ability to better monitor and control energy consumption (Kothari, 2015; Lee & Seshia, 2011). For industry, IoT supports increasing process control that assists the implementation of new more integrated business models. Reflecting these benefits, business is adopting IoT at pace (Goodness et al., 2019). Business drivers cited in press releases and industry white-papers as underpinning the decision to invest in industrial variants of IoT technologies range from increasing productivity, mitigating occupational health and safety considerations, standardisation of quality and performance, and to address the challenges of aging work forces amongst others. Examples of business IIoT implementations are presented in Appendix 1 which sets out the initiatives of Rio Tinto, Billerud Korsnas AB, NSW State Rail, Yara Birkeland AS, Coles Supermarkets, Amazon, Port of Rotterdam, and NASA.

However, much of the research in respect of IoT design is focused on implementation specific applications, with design frameworks or methodologies at an overarching strategy level receiving a light touch in literature. Additionally,

much of the literature about IoT system security fails to take account of IoT's hybrid characteristics. Traditionally data security in *Information Technology* (IT) systems has been viewed through the prism of the CIA triad as shown in **Figure 1** which places confidentiality at its apex, followed by data integrity and availability (Gordon, 2015; Integra Technical, 2019; ISACA, 2015). The *Operational Technology* (OT) systems that underpin critical infrastructure inverts the triad and places availability and integrity at the apex, followed by confidentiality. However, implementations of IoT and *Industrial IoT* (IIoT) represent a fusion of traditional IT and OT.

Figure 1: IT Security Triad supporting OT

This paper discusses the nature of IoT and how profession-based training will need to develop to meet the desired levels of IoT functionality with an emphasis on the design of secure IoT systems.

In the following section we consider industrial usage, as well as the distributed nature of IoT development which creates real challenges for the education and training models necessary to support robust IoT security.

Review Industrial Use-Cases

Forecasts around the number of IoT connected devices are extremely bullish and project 50.1 billion connected units globally by 2020, up from 18.2 billion in 2015 (Steden & Robert Kirchner, 2018). As the uptake of devices grows the connection surface that this plethora of devices can join in either an ad-hoc personal, an ad-hoc community, or industrial ecosystems will increase exponentially. Cisco (2019) forecast that industrial type machine-to-machine (M2M) connections will account for 48 percent of all IoT connected devices by 2022. Figure 2 shows that M2M implementations are tipped to total 14.6 billion connections in 2022, an average of 1.8 Machine-to-Machine (M2M) connections per person globally (Cisco, 2019, p. 11).

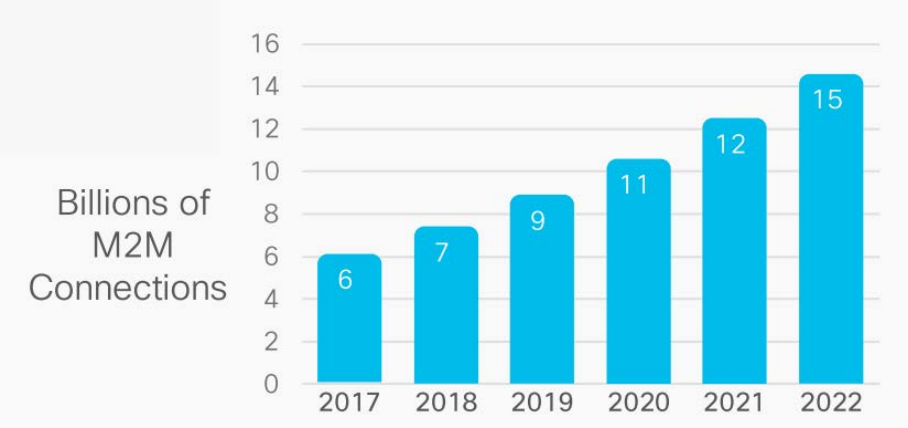


Figure 2: Projected M2M connection growth globally

This increasing uptake of IoT devices across a range of use-cases, such as those shown in Appendix 1, creates significant security risk as deployments create a large number of backdoors for potential attackers, while power consumption in resource constrained devices, as well as market pressure for competitive pricing limits traditional security protections like firewalls and cryptography (Alioto, 2017).

The National Institute of Technology (NIST) defines IoT as combining "*sensing, computing, communication, and actuation*" to form distributed smart systems (Voas, 2016). Particularly in industrial settings the *smart* factor enables businesses to automate tasks to increase productivity, simplify human resource (HR) management, and ensure operating consistency. Many of these industrial implementations view IoT security through the lens of *Operational Technology* (OT), thereby prioritising system availability over data confidentiality as system failure risks human injury or potentially loss of life. OT security has historically relied on *air-gapped* networks separated from other domains and the Internet, to provide confidentiality as well as data integrity. However, increasingly to drive business value from IIoT systems, businesses are connecting these distributed smart systems to *Enterprise Resource Planning* (ERP), as well as other business systems to provide managers with a more comprehensive view of asset performance (Desai, 2016; Flammini, 2019). The more system connection points there are, the greater the surface that could result in security failings.

Appendix 1 sets out examples of recent IoT implementation by industry, as well as summarising some of the business drivers that spurred the investment in these smart systems.

The IoT ecosystems supporting the industrial use-cases set out in Appendix 1 are a heterogenous structure of hardware devices, with software supporting distributed operations that utilise:

- Cloud
- Edge computing
- Sensor and actuator nodes (Isakovic et al., 2018)
- Artificial Intelligence for near real time decisioning

Edge computing assists this real time decisioning as having computational processing completed close to the source of the sensors reduces latency resulting from data being sent over the cloud, processed, and the resulting instructions returned to the device's actuators for execution. The skills necessary to optimise these implementations are varied, with the required knowledge drawing from multiple highly technical domains. Embedded systems such as those used in IoT devices will comprise microcontrollers, and subject to the device's required functionality could include microprocessors. As microprocessors deliver greater computational power they require operating systems and program memory such as RAM (Kothari, 2015), whereas microcontrollers are effectively a micro-computer on a single integrated circuit but are resource constrained with limited capability (Lee & Seshia, 2011, p. 177). Microcontrollers are also increasingly being adapted to support edge devices by vendors such as Arduino, ARM, Raspberry Pi and Intel Galileo among others (Bloom, Alsulami, Nwafor, & Bertolotti, 2018, p. 3). At a component level the investments by these manufacturers of microcontrollers in extending device capability, as well as the implementation specific investments in IIoT by industry (as set out in Appendix 1), helps to illuminate the broader trends in IoT. However, while significant volumes of literature deal with the direction of education at a device, or IoT implementation level, references in literature that deal explicitly with education and training of secure design are limited. For example the comprehensive review of microcontroller education by Bolanakis (2019) only mentions security once, and the only references to "*secure*" is made in the context of digital (SD) cards (p. 50). Yet robust security is at the core of the functional benefits that the developer of IoT devices have premised end-user uptake of the device upon in the first instance.

As well as more powerful microcontrollers, rapid IoT prototyping systems incorporating modular componentry and easy to use integrated development environments (IDE), have become more accessible. Examples of rapid IoT prototyping systems include the vendors listed above such as Arduino and Raspberry Pi. Supporting IoT developer use of these rapid prototyping systems is the significant volume of do-it-yourself free instructional content available online, which supports outcome focused IoT functionality. However, a secure outcome may not always be achieved unless security is prioritised and considered from the commencement of the design process.

Citing the economist Kenneth Galbraith in respect of business strategy, Ansoff, Kipley, Lewis, Helm-Stevens, and Ansoff (2019, p. 64) observe that for industry change is a continuum as technological innovation drives new business models leading to changing relationships between organisations, customers and governments (Ansoff et al., 2019, p. 64). Applying Galbraith's observations to education and training, education providers control of training content and certification is challenged by the ease of access to free training content. More troubling in relation to the focus of this paper is that readily available do-it-yourself IoT prototyping training contains almost no reference to secure design.

Citizen Prototyping

IoT implementation relies on the coordination of hardware, firmware, and software with the extent of interaction referred to in technology terms as *coupling* (Gordon, 2015; Törngren & Sellgren, 2018). Lower coupling is considered better because objects are more independent, simplifying troubleshooting and updating, but Törngren and Sellgren (2018) identify that IoT and its derivatives are tightly coupled because the systems are combined to support an integrated business process. Typically, multidisciplinary projects are managed under an integrated structure. An example of a formal project methodology is PMBOK developed by The Project Management Institute [PMI] (2012), which is directed at supporting project governance as the project progresses through its progressive stages. Software development is often characterised by the sequential or overlapping stages of the Waterfall project method. Some scholars advocate that by including security consideration throughout the *System Development Life Cycle* (SDLC) that more robust security architecture results (Whitman & Mattford, 2018).

A less structured development method is the Agile project methodology, which favours working software over documentation. Originally developed as an alternative to the process driven approach, Agile advocates iterative working

models and customer collaboration to deliver incremental improvements in software (Beck et al., 2001). Agile has increased in popularity in recent years such that it is now commonly utilised in rapid development across both citizen prototyping, as well as the full life-cycle management of IoT devices. While in broad terms the most common process and design methods/frameworks approximate what is required to manage development of IoT devices using embedded systems and communication networks, security is not explicitly included in these models. Illustrating the issues facing secure design, supporting citizen prototyping are websites like *If This Then That*, or IFTTT (ifttt.com) which has available a library of applets many developed by citizen programmers, including those for use in IoT devices. However, highlighting poor security design Lodge, Crabtree, and Brown (2018) found that 50% of the samples they analysed drawn from the approximately 20,000 applets on IFTTT contained confidentiality or integrity violations.

In this section we have noted the extent to which industry and business models are adapting to utilise IoT. With IoT representing a fusion of IT and OT, new security models are needed. Perhaps rather than using the term *Internet of Things* or IoT, adopting the name *Information Operational Technology* or IOT would more accurately describe the technology, and better inform thinking around training and education. While IOT speaks to the target state for security education and training, the fragmentation of educational content not bound by formal authorities or standards, as well as the trend towards speed to market strategies focused on acquiring market share, challenges the linear design and delivery of traditional technology and security education.

The following section sets out the research methodology used, followed by a discussion of key findings, and by the conclusions of this research.

RESEARCH METHODOLOGY

The challenge for the education sector is to ensure it provides the appropriate level of training to support the development and maintenance of these complex IoT systems. In considering what factors in IoT could frame an appropriate syllabus, Taivalsaari and Mikkonen (2018) identify six distinct components in defining a IoT taxonomy as:

- Energy consumption.
- Hardware capability and cost.

- Software development.
- Isomorphic architectures supported by virtualisation and containerisation.
- Edge computing.
- Interoperability in the absence of specific standards (pp. 86-87).

Adapting the taxonomy of Taivalsaari and Mikkonen (2018), this research created a three stage process to identify broadly the extent to which these IoT components are consisdered in the context of teaching *secure design*. The key word criteria was summarised in two blocks. Graphically, Figure 3 shows the bounding of the key words adopted in the first part of this research criteria.

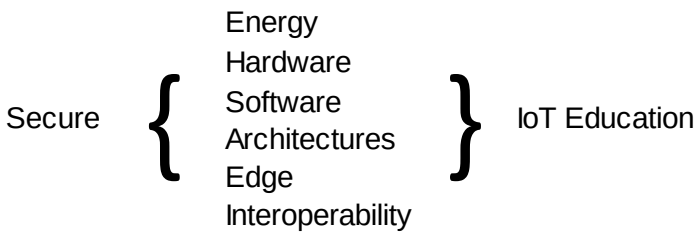


Figure 3: Initial search criteria

Reflecting process governance, Figure 4 includes as criteria Project Management to bring governance to design methods in support of secure design and therefore, reliable IoT operating states.

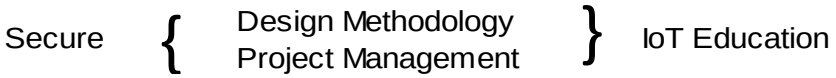


Figure 4: Additional search criteria

With Figure 3 and Figure 4 showing the key words identified, to ensure the maximum number of results were returned we used the Boolean operator “AND” in conjunction with our keywords. The results were processed through a funnel of successive refinement to reduce the initial number of 4,980 results (which will include significant duplication) down to 95 papers, which were then critically reviewed. To illustrate the process refinement utilised, Figure 5 shows the progressive filtering applied adopting the visual presentation style used by Bilal, Gani, Lali, Marjani, and Malik (2019).

The filtering process followed an intuitive methodology in reducing the number of abstracts reviewed (N = 262) before full texts were screened (N = 100), noting that arriving at the 262 articles had been the product of Boolean searches in the first instance against the peer reviewed IEEE and Reed Elsevier databases as shown in Appendix 2 (Nickerson, Varshney, & Muntermann, 2013). Finally, five articles were removed owing to their publication dates preceding 2017 despite the publication period of 2018 through current being part of the selection criteria, as well as some results being indexes and not complete papers. This final step reduced the number of full texts to give N = 95.

Wang, Myers, and Sundaram (2013) set out a number of processes in completing literature reviews that include search string validation. To that end we reviewed a paper from the proceeding of the *23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* by Burd et al. (2018). The work of Burd et al. (2018) is relevant in the context of this paper, in that Burd et al. propose a *Model Transdisciplinary IoT Curriculum*, characterised by instructors mastering 15 modules over 10 distinct disciplines including computer science design.

However, the work of Burd et al. (2018) has deliberately excluded as it is published in journals, books and conference proceedings devoted to information security education. The reason for excluding such papers is to better understand how other stakeholders see IoT education, thereby more broadly informing the challenges IoT education will need to address. For example, a paper by the researchers Tuptuk and Hailes (2018) stresses the critical role of education in secure IoT supported manufacturing processes, but the paper appears in *The Journal of Manufacturing Systems* not in an education focused journal. Or the paper of Kozák, Ružický, Štefanovič, and Schindler (2018) titled *Research and Education for Industry 4.0* being included in the *2018 Cybernetics & Informatics* conference. On that basis the work of Tuptuk and Hailes (2018) and Kozák et al. (2018) is included in our findings.

The rationale for excluding research published in information security education specific sources, was when initially defining the research question it was observed much of the research in the education domain focuses on IoT as the enabling infrastructure. But, the purpose of this research is to understand how foundational concepts like secure design are seen more broadly in the context of IoT education.

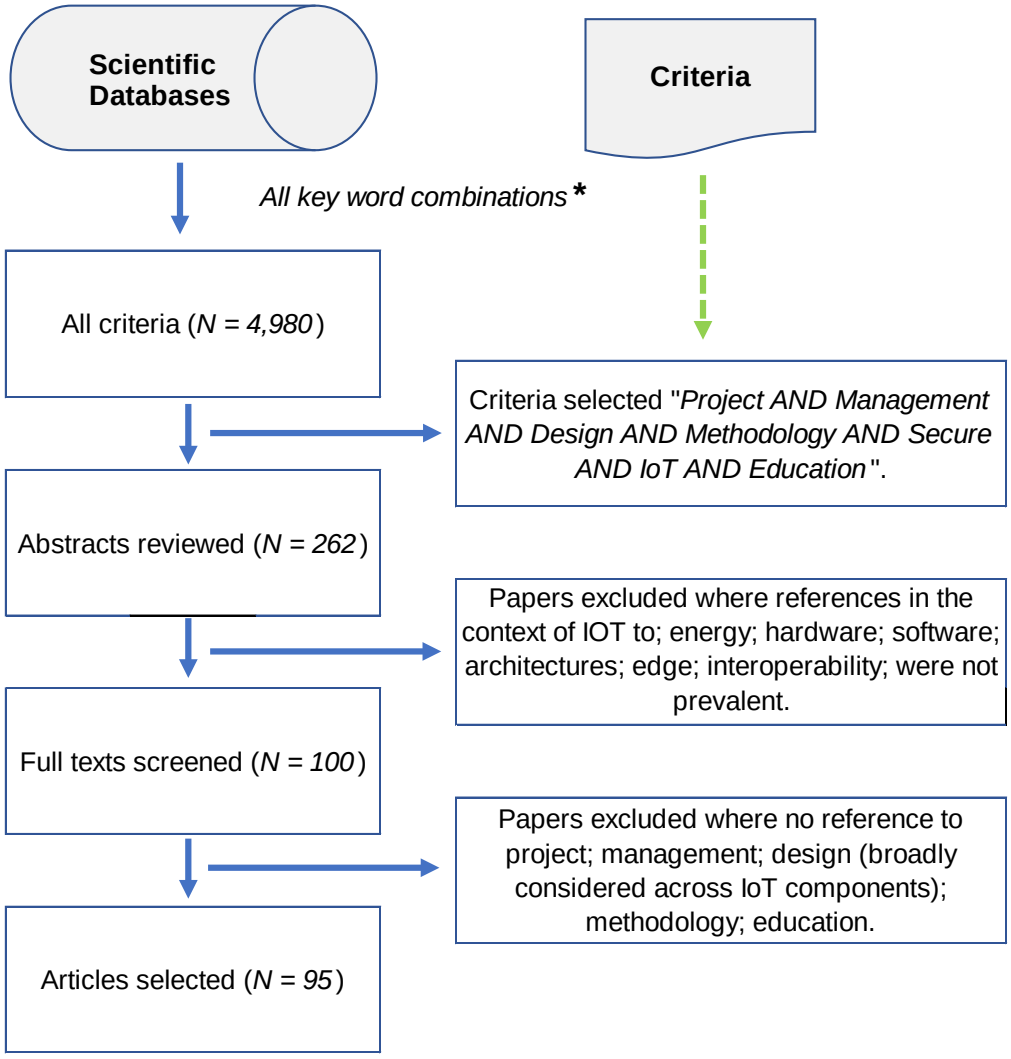


Figure 5: Key inclusion criteria

DISCUSSION

Our review was not limited solely to the papers title, its abstract, and introduction, rather the complete paper was analysed. In all, approximately 60 words were used

to categorise the prevalent themes identified in the 95 papers. All 60 words were related to the key word criteria set out in Figure 3 and Figure 4 above, whether individually as words, or in the round, the discussion in literature they addressed. Appendix 3 lists the top 25 themes, which account for 90% of the terms used in the categorisation process. In respect of categorising papers, either IoT or IIoT was selected on a largely distinct basis, although 8% of papers had addressed both the broader topics associated with IoT and Industrial IoT in sufficient depth it was considered appropriate to categorise them both as being IoT as well as IoT focused.

To bring some granularity to the keyword process, Appendix 4 summarises the detailed analysis of 10 of the 95 articles critically reviewed, including keywords/themes identified.

Appendix 3 illustrates the trend that increasingly because of IoT the traditional model of IT with defined networks bound by authentication; authorisation; accountability; to support confidentiality, are now merging with OT networks where traditionally isolated networks are used to support high system availability and integrity of the data flowing across them. The authors of this paper postulate that rather than IoT this fusion of information and operational technologies more approximates IOT representing Information Operational Technologies.

Critical in ensuring a quality of service across IoT devices which satisfies; confidentiality; integrity; availability; but where these concepts shift interchangeably by implementation, a more considered ground up approach to secure design is required. To understand the current trends, Appendix 1 set out examples of IIoT adoption by industry illustrating the increasing trend towards automation of industrial processes using IoT technologies. Given these trends, this research found that broadly literature dealing with IoT education is fragmented. For example, summarising 10 of the 95 papers reviewed as shown in Appendix 5 found the following disparate themes;

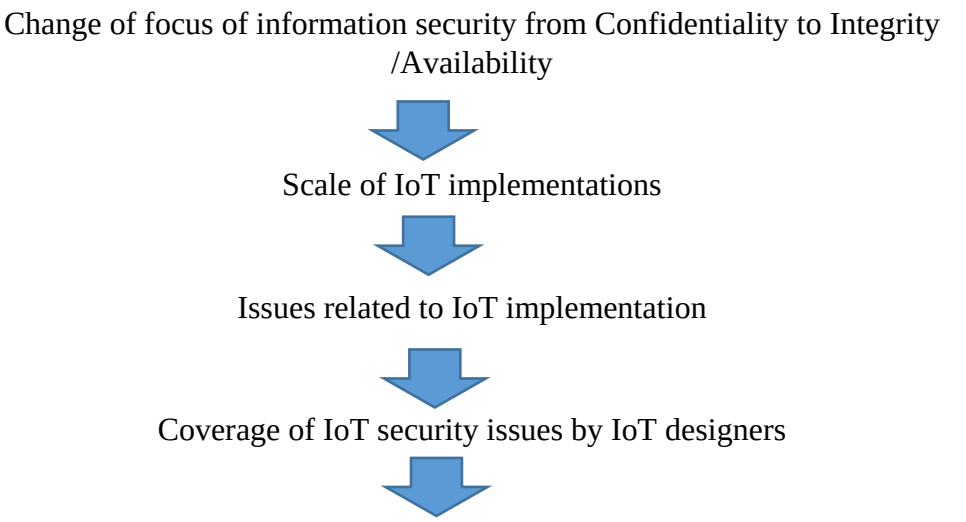
- Industry specific implementations such as the electricity grid, or other industrial implementations;
- Operational implementations such as the use of block chain in for example IoT e-health applications;
- Component specific developments around maximising microcontroller and microprocessor performance;

- While citizen prototyping is well considered in literature, explicit references to the security needed in the IoT systems being modelled are lacking;
- Where references to secure design are made, they are typically in the context of microcontrollers and microprocessors.

While these 10 papers included in Appendix 4 are in the opinion of the authors of this paper excellent, themes linking education in respect of secure IoT design, and education covering secure IoT integration, are not prevalent.

CONCLUSION

Illustrating the logical sequence used to consider the issues in literature around IoT and IIoT security:



These needs are based on our finding that there are no papers which explicitly stated education in the context of secure design focused on information security across the concept of IOT as introduced in this paper. Yet information security is at the core of the automated decisioning that many of the current IoT systems are designed to support.

These findings indicate that despite numerous education specialists calling for IoT training to better address security issues, these efforts are not reflected in industry centric publications.

In our next research phase, we plan to study developments around the systems approach related to IOT systems design.

REFERENCES

Alioto, M. (2017). *Enabling the Internet of Things : from integrated circuits to integrated systems* (Vol. 282 ~). Cham, Switzerland: Springer.

Ansoff, H. I., Kipley, D., Lewis, A. O., Helm-Stevens, R., & Ansoff, R. (2019). *Implanting strategic management*. Cham, Switzerland: Palgrave Macmillan, Cham.

Beck, K., Beedle, M., Van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., . . . Jeffries, R. (2001). Manifesto for Agile Software Development Retrieved from agilemanifesto.org

Bilal, M., Gani, A., Lali, M. I. U., Marjani, M., & Malik, N. (2019). Social Profiling: A Review, Taxonomy, and Challenges. *Cyberpsychology, Behavior, and Social Networking, 22*(7), 433-450. doi:10.1089/cyber.2018.0670

Black, T. (2019). Robots Edge Closer to Unloading Trucks in Amazon-Era Milestone. *Hyperdrive*. Retrieved from www.bloomberg.com/news/articles/2019-05-03/robots-edge-closer-to-unloading-trucks-in-amazon-era-milestone

Bloom, G., Alsulami, B., Nwafor, E., & Bertolotti, I. C. (2018, 13-15 June 2018). *Design patterns for the industrial Internet of Things.* Paper presented at the 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS).

Bolanakis, D. E. (2019). A Survey of Research in Microcontroller Education. *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje, 14*(2), 50-57. doi:10.1109/RITA.2019.2922856

Burd, B., Barker, L., Pérez, F. A. F., Russell, I., Siever, B., Tudor, L., . . . Pollock, I. (2018). *The internet of things in undergraduate computer and information science education: exploring curricula and pedagogy.* Paper presented at the Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education.

Cisco. (2019). *Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper*. Retrieved from www.cisco.com: www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf

Desai, N. (2016). IT vs. OT for the Industrial Internet – Two Sides of the Same Coin? Retrieved from www.globalsign.com/en/blog/it-vs-ot-industrial-internet/

Flammini, F. (2019). *Resilience of cyber-physical systems : from risk modelling to threat counteraction*: Cham, Switzerland : Springer. 2019.

Goodness, E., Kim, S., Friedman, T., Velosa, A., Berthelsen, E., & Shrivastava, A. (2019). *Magic Quadrant for Industrial IoT Platforms*. Retrieved from Stamford, USA: www.gartner.com/document/3941962?ref=solrAll&refval=227511840&qid=d78da79f3d597e73a88675

Gordon, A. (2015). *Official (ISC)2 guide to the CISSP CBK* (Vol. Fourth Edition). Boca Raton, Florida, USA: Auerbach Publications.

Gray, D. (2019, 27 April 2019). No one behind the wheel: The new workforce driving Australia's mines. *Sydney Morning Herald*. Retrieved from www.smh.com.au/business/companies/no-one-behind-the-wheel-the-new-workforce-driving-australia-s-mines-20190411-p51dd2.html

Hastie, H. (2019, 16 June 2019). No more training wheels: Rio Tinto launches 'world's biggest robot'. *Sydney Morning Herald*. Retrieved from www.smh.com.au/business/companies/no-more-training-wheels-rio-tinto-launches-world-s-biggest-robot-20190614-p51xxj.html

Hatch, P. (2019, 26 March 2019). Coles brings in robot supermarket Ocado for online overhaul. *Sydney Morning Herald*. Retrieved from www.smh.com.au/business/companies/coles-brings-in-robot-supermarket-ocado-for-online-overhaul-20190326-p517je.html

Integra Technical. (2019). Framing Cyber Risk. In: Integra Technical Services.

ISACA. (2015). *Cybersecurity Fundamentals Study Guide*. Rolling Meadows, IL 60008, USA: ISACA.

Isakovic, H., Ratasich, D., Hirsch, C., Platzer, M., Wally, B., Rausch, T., . . . Dustdar, S. (2018). *CPS/IoT Ecosystem: A platform for research and education.* Paper presented at the Proceedings of the 14th Workshop on Embedded and Cyber-Physical Systems Education (WESE 2018), Turin, Italy.

Kothari, D. P. (2015). *Embedded Systems* (Second edition. ed.). London, WC1N 3AX, UK: New Academic Science.

Kozák, Š., Ružický, E., Štefanovič, J., & Schindler, F. (2018, 31 Jan.-3 Feb. 2018). *Research and education for industry 4.0: Present development.* Paper presented at the 2018 Cybernetics & Informatics (K&I).

Lee, E. A., & Seshia, S. A. (2011). *Introduction to Embedded Systems : A Cyber-Physical Systems Approach* (First. Printing 1.08 ed.). Berkeley, CA, 94720-2284, USA: UC Berkeley

Lodge, T., Crabtree, A., & Brown, A. (2018). *IoT App Development: Supporting Data Protection by Design and Default.* Paper presented at the Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers, Singapore.

NASA. (2019). Spinoff 2019. *NASA Technology Transfer Program*. Retrieved from spinoff.nasa.gov/Spinoff2019

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems, 22*(3), 336-359. doi:doi.org/10.1057/ejis.2012.26

O'Sullivan, M. (2019). Sydney metro line expected to open week after federal election. [22 May 2017]. *Public Transport*. Retrieved from www.smh.com.au/national/nsw/sydney-metro-line-expected-to-open-week-after-federal-election-20190503-p51joy.html

Paris, C. (2019). Rules for Robot Cargo Ships Could Be Years Away, Regulator Says. *Logistics Report*. Retrieved from www.wsj.com/articles/rules-for-robot-cargo-ships-could-be-years-away-regulator

Port of Rotterdam. (n.d.). The robot is coming. Retrieved from www.portofrotterdam.com/en/doing-business/logistics/cargo/containers/50-years-of-containers/the-robot-is-coming

Project Management Institute [PMI]. (2012). *PMI Lexicon of Project Management Terms* (2 ed.). Newtown Square, Pennsylvania 19073-3299, USA: Project Management Institute.

Starn, J. (2019). Robots Thrive in the Forest on Jobs That Humans Find Too Boring. *Technology*. Retrieved from www.bloomberg.com/news/articles/2019-01-09/u-s-deploys-new-tactics-in-prosecution-of-chinese-chipmaker

Steden, P., & Robert Kirchner, R. (2018). Industry 4.0 – Overview and Policy Implications. In G. A. G. B. Economics (Ed.). Berlin, Germany: German Advidory Group Ukraine

Taivalsaari, A., & Mikkonen, T. (2018). A Taxonomy of IoT Client Architectures. *IEEE software*, *35*(3), 83-88. doi:10.1109/MS.2018.2141019

Törngren, M., & Sellgren, U. (2018). Complexity Challenges in Development of Cyber-Physical Systems. In M. Lohstroh, P. Derler, & M. Sirjani (Eds.), *Principles of Modeling: Essays Dedicated to Edward A. Lee on the Occasion of His 60th Birthday* (pp. 478-503). Cham: Springer International Publishing.

Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, *47*, 93-106. doi:doi.org/10.1016/j.jmsy.2018.04.007

Voas, J. (2016). Networks of 'things'. In *NIST Special Publication 800-183* (Vol. SP 800-183, pp. 800-183). Gaithersburg, MD 20899-8930, USA: NIST.

Whitman, M. E., & Mattford, H. J. (2018). *Principles of information security* (Sixth ed.). Boston, MA 02210, USA: Cengage Learning.

APPENDIX 1

Examples of IIoT adoption by industry.

Industry	Business Driver	Application	Enterprise	Location
Mining	Flexibility and efficiency.	Autonomous trains	Rio Tinto	Automated trains moving iron ore from mines located in Australia's Pilbra to costal ports along Rio's 1,700 km privately own railway (Hastie, 2019).
Mining	Scale of operations and repetitive nature of work.	Autonomous trucks	Rio Tinto	240 autonomous trains traveling at up to 60kms an hour to move iron ore from the mine pits to the train loading facility (Gray, 2019).
Primary Industry	Scale of, and repetitive nature of task.	Decision making	Billerud Korsnas AB	AI analyses thousands of diagrams to determine just how long is needed to cook wood chips before they turn into pulp (Starn, 2019).
Public Transport	Simplification of training and HR.	Consistency and extended operation	NSW State Rail	Australia's NSW state government introduces driverless passenger trains onto Sydney's metropolitan train network (O'Sullivan, 2019).
Shipping	Cost savings.	Autonomous coastal shipping	Yara Birkeland AS	Targeting go-live in 2020 the 120-container ship will ply Norway's waters. At US$20 million the cost is 3 times a conventional ship, but will cut operating costs by 90% (Paris, 2019).
Logistics	Efficiency gains.	Scale up operations	Coles Supermarkets	The Australian grocery retailer has partnered with the UK company Ocado, to implement Ocado's autonomous warehouse systems for the selection and packing of home delivery orders (Hatch, 2019).
Logistics	Elimination of miserable tasks.	Loading and unloading truck trailers	Amazon	Siemens and Honeywell devices work at approximately the same rate as humans. Equipped to handle the complexity of human decisioning around parcels of many differing spatial dimensions and weights.

				Working inside a trucks trailer labelled as a "*miserable*" task (Black, 2019, p. 1).
Logistics	Elimination of dangerous and repetitive tasks.	Loading and unloading of container shipping, and dispatch from port.	Port of Rotterdam	Automated container cranes extend autonomous functional of APMT and RWG container terminals at the Port to provide largely autonomous operations, and when required can be guided by remote operators (Port of Rotterdam, n.d.)
Hazardous environments	Hazardous environments; disaster relief to the oil and gas industry.	Replicate range of human movement	Awaiting implementations	Nasa's RoboMantis with four legs on wheels and either one or two arms capable of wielding various tools, the robot is intended to carry out jobs that are hazardous to humans (NASA, 2019, pp. 66-69).

APPENDIX 2

Search Criteria	IEEE Explore							
	Journals	**Conferences**	**Courses**	**Magazine**	**Book**	**Standard**	**Total**	**%**
Energy AND Secure AND IoT AND Education	269	668	1	95	77	10	**1,234**	*96%*
Hardware AND Secure AND IoT AND Education	6	5	1	1	0	0	**13**	*1%*
Software AND Secure AND IoT AND Education	9	7	1	0	0	0	**17**	*1%*
Architectures AND Secure AND IoT AND Education	7	7	1	0	0	0	**15**	*1%*
Edge AND Secure AND IoT AND Education	0	0	0	0	0	0	**-**	*0%*

Interoperability AND Secure AND IoT AND Education	0	0	0	0	0	0	-	*0%*
Energy AND Hardware AND Software Architectures AND Edge AND Interoperability AND Secure AND IoT AND Education	0	0	0	0	0	0	-	*0%*
Design AND Methodology AND Secure AND IoT AND Education	1	1	1	0	0	0	**3**	*0%*
Project AND Management AND Secure AND IoT AND Education	5	1	1	0	0	0	**7**	*1%*
Project AND Management AND Design AND Methodology AND Secure AND IoT AND Education	0	0	1	0	0	0	**1**	*0%*
Total	**297**	**689**	**7**	**96**	**77**	**10**	**1,290**	**100%**

Search Criteria	**Reed Elsevier (Science Direct)**					
	2017	**2018**	**2019**	**2020**	**Total**	**%**
Energy AND Secure AND IoT AND Education	113	181	252	6	**552**	14%
Hardware AND Secure AND IoT AND Education	90	140	186	2	**418**	10%
Software AND Secure AND IoT AND Education	138	213	279	6	**636**	16%
Architectures AND Secure AND IoT AND Education	118	186	275	7	**586**	14%
Edge AND Secure AND IoT AND Education	64	107	164	3	**338**	8%
Interoperability AND Secure AND IoT AND Education	58	74	106	1	**239**	6%
Energy AND Hardware AND Software Architectures AND Edge AND Interoperability AND Secure AND IoT AND Education	14	22	20	31	**87**	2%

Design AND Methodology AND Secure AND IoT AND Education	76	129	178	4	**387**	*10%*
Project AND Management AND Secure AND IoT AND Education	104	193	254	3	**554**	*14%*
Project AND Management AND Design AND Methodology AND Secure AND IoT AND Education	29	96	135	2	**262**	6%
Total	**804**	**1,341**	**1,849**	**65**	**4,059**	**100%**

APPENDIX 3:

Count of most frequent groupings.

Ref	Term	Count	Ratio		Ref	Term	Count	Ratio
1	IoT	75	13%		**14**	framework	9	2%
2	security	69	12%		**15**	secure	9	2%
3	architecture	62	11%		**16**	citizen programming	8	1%
4	design	37	7%		**17**	implementation specific	8	1%
5	education	35	6%		**18**	business models	7	1%
6	IIoT	28	5%		**19**	business models	7	1%
7	training	21	4%		**20**	education delivery	5	1%
8	communication protocols	20	4%		**21**	cloud	5	1%
9	cyber physical systems	19	3%		**22**	integrity	5	1%
10	operational optimisation	17	3%		**23**	microcontroller	5	1%
11	privacy	15	3%		**24**	microprocessor	5	1%
12	Industry 4.0	14	3%		**25**	secure implementation	5	1%
13	blockchain	13	2%					

APPENDIX 4

Examples of articles selected.

Paper	Title	Keywords / Themes	Characteristics
Faheem et al. (2018)	Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges	secure; operational; IT; education; Industry 4.0	Discusses operational processes that require integration, but makes no explicit reference to OT. Industry specific optimisation is discussed in the context of smart electricity. Education is referenced in the context of future partnerships between educational providers and the energy industry.
Khattak, Shah, Khan, Ali, and Imran (2019)	Perception layer security in Internet of Things	citizen programming; security controls; communication protocols; architecture; security	Uses perception layer as the collection mechanism close to the implementation of sensor noting the perception layer is responsible for data collection and data transmission for further processing. Considers countermeasures necessary for robust implementation in terms of protecting the business model. While it does not explicitly reference secure design observes that more complex circuits need to be designed to ensure attacks like side-channel attacks, cannot be launched.
Kozák, Ružický, Štefanovič, and Schindler (2018)	Research and education for industry 4.0: Present development	IIoT; cyber physical systems; architecture; education design; integration	Presents state-of-the-art in research and education, propose a main master study courses include; Security in Indus*try* but no specific reference to secure design. Notes that one of the future educational theme in Industry 4.0 that will need to be addressed is *Security in Industry*, which would prima facie approximate IOT introduced as a concept in the introduction to this paper.
Xu et al. (2018	A Security Design for the Detecting of Buffer Overflow Attacks in IoT Device	embedded; security design; architecture; microprocessors; operational optimisation	Proposes an architecturally enhanced security hardware design to detect buffer overflow attacks. Includes instructions monitoring and verification used to trace the execution behaviour of programs. Additionally, proposes a secure tag validation to monitor the attributes of every memory segment. At run-time, the designed hardware observes its dynamic execution trace and checks whether the trace conforms to the permissible behaviour, if not response mechanisms will be triggered. While secure design is not explicitly stated as a term within the paper it is the main theme of the paper.

Tuptuk and Hailes (2018)	Security of smart manufacturing systems	IIoT; industry 4.0; geo-political; operational optimisation; security; architecture	In an Industry 4.0 context this work notes standardisation, education and law/regulation are key enabling factors to achieving system security in the manufacturing industry. Draws the distinction between manufacturing and IT systems so approximates the merger between IT and OT. Notes that in terms of system security the move to industry implementing commercial-off-the-shelf (COTS) technologies provides significant volumes of literatures for threat-actors to use in identifying vulnerabilities in manufacturing platforms.
Wang, Ali, Guin, and Skjellum (2018)	IoTCP: A Novel Trusted Computing Protocol for IoT	resilience; trust; security; IIoT; cyber physical systems; IoBT	Trusted computing protocol that employs discrete Trusted Platform Modules (TMP) and Hardware Security Modules (HSM) for key management, a blockchain-based package verification algorithm for over-the-air security, and a secure authentication mechanism for data communication. The resulting solution propose integrates hardware security, strong cryptographic hash functions, and peer-based blockchain trust management in support of operational technologies.
Raikar, Desai, Vijayalakshmi, and Narayankar (2018)	Upsurge of IoT (Internet of Things) in engineering education: A case study	education delivery; architecture; citizen programming; education content; framework	Education content that approximates the 5 levels identified by Taivalsaari and Mikkonen (2018) referred to in this paper, plus the addition of Level-6 that include '*prediction*' which the authors of this paper read to be in support of AI decisioning. Security is discussed more at a conceptual level.
Werner, Schilling, Unterluggauer, and Mangard (2019)	Protecting RISC-V Processors against Physical Attacks	security; microcontroller; architecture; confidentiality; microprocessors	Considers microcontroller implementations of RISC-V, an emerging instruction-set architecture where one of the main security risks is attackers having direct physical access to the microchip. While secure design is not explicitly stated within the paper it is the main theme of the paper.
Luca, Li, Mian, and Chen (2018)	Visual programming language environment for different IoT and robotics platforms in computer science education	IIoT; fog; cyber physical systems ;architecture; education content; simulation	A visual programming language that supports the integration of engineering design process, workflow, fundamental programming concepts, control flow, parallel computing, event-driven programming, and service-oriented computing from introduction through increasing student competencies. It supports simulation environments and actual physical devices in a classroom environment. The term *security* is not used in the paper, with *secure* referenced twice in the context of *web services*.
Thorburn, Margheri, and Paci (2019)	Towards an integrated privacy protection framework for IoT: contextualising regulatory requirements with industry best practices	IIoT; cyber physical systems; resilience; education delivery; body of knowledge	Overarching design criteria. Relevant in the context of this paper as we have looked at use-cases and in many consumer facing IoT implementations in particular privacy and trust may provide barriers to consumer adoption. Additionally, for developers the fines imposed on controllers under GDPR impose material fines. Also, the research of Burd et al. (2018) includes B*usiness Management* and *Business Essentials* as two of the distinct disciplines.