# IoT Security: Challenges and Solutions for Mining

Glenn Barrie
School of Engineering
Curtin University
Kent St, Bentley WA 6102
+61 8 9266 9266
Glenn.Barrie@postgrad.curtin.edu.au

A/Prof. Andrew Whyte
School of Engineering
Curtin University
Kent St, Bentley WA 6102
+61 8 9266 9266
Andrew.Whyte@curtin.edu.au

Dr. Joyce Bell
School of Engineering
Curtin University
Kent St, Bentley WA 6102
+61 8 9266 9266
Joyce.Bell@curtin.edu.au

## ABSTRACT

The Internet of Things (IoT) paradigm with its vast range of heterogeneous connecting technologies heralds a new era for internet research, especially given that this explosion in connectivity for devices or 'things' is not without risk. Scholars recognise that IoT security concerns persist and that evidence highlighting increasing cyber-security vulnerabilities requires attention. Currently IoT security literature confirms: industry confusion, lack of clear standards, interoperability fears and security problems (with reference to identity, authentication, access control, protocol and network security, privacy, and trust and governance difficulties all within the IoT technology realm). In short, there is urgent need for governance in IoT to avoid unstructured fragmentation of architectures, protocols and identification systems, and responsibilities. To address anticipated future numbers of IoT devices, a secure, scalable, yet flexible solution is needed to work across a range of technologies and dynamic environments. Specific industries such as the Western Australian (WA) Mining and Resource sector, whilst recognised as an early adopter of technology/ IoT applications, is also currently seeking security solutions that provide competitive advantage. To this end, the research being conducted here is utilising qualitative methodologies (alongside document analyses), and specific real-world/live case-studies towards relevant organisations' IoT cyber-security decision making, with a view to developing best-practice cross-party guidance(s). Work here is at its early stages; ultimately variables identified and subsequently validated shall go towards a new developed design guide for the deployment of Information Technology/ Operational Technology and IoT environments, to address IoT security concerns, applicable to (major WA mining and resources companies and) the energy and resources generally.

## Keywords

IoT security; OT security; cyber-security; mining-industry; Western-Australian resources-industry; disruptive technologies.

## 1. INTRODUCTION

In recent years, there has been a rapid uptake of converging both Information Technology (IT) and Operational Technology (OT) environments as organisations seek to improve their bottom line by reducing costs [25]. Now with the evolving world of connected Internet of Things (IoT), these same businesses are fast identifying the new global advantages that IoT may bring to international and competitive markets. The resources and mining industry in Western Australian (WA) is a case in point.

Mining in the resource rich state of WA is of great importance, largely due to the enormous economic benefits it brings. The mining industry, in WA alone, added AUS$79 billion (US$60 billion) to state government revenue in 2013-14 [33]. This value was more than 5% of Australia's total Gross Domestic Product (GDP). Therefore, any potential disruption or impact to this sector could have devastating economic and potentially safety repercussions; thus any deployment(s) of the IoT used for mining must be delivered safely, to a standard and be made secure.

One of the major advantages the IoT brings to mining is the ability to aid the optimisation of the digital supply chain [21] through the introduction of disruptive-technologies like the IoT, rather than relying on traditional optimisation of the physical supply-chain that can sometimes be cost prohibitive.

This observation is supported anecdotally; the author, as the Technology-Lead working for a tier one global mining company in WA, is leading projects already seeking to introduce private Long Term Evolution (LTE or 4G) as the next generation wireless solutions across the company's global operations. This enterprise LTE (eLTE) network is acting as an enabler or platform for further disruptive technologies such as data analytics (big data), that the company can then leverage to unlock further value from their (iron ore) assets, by not only increasing productivity and safety, but also provide a much needed platform for the future of mining-autonomy.

For mining companies to achieve these types of productivity goals and efficiencies, using advanced wireless platforms like eLTE, they will also need to consider their strategy for the IoT. The IoT is considered the next significant evolution of the internet; its main

components include Radio Frequency IDentification (RFID) tags, actuators, human wearables (activity trackers that are wireless-enabled wearable technologies) and of course the sensors, which are already in abundance within the mining industry and primarily used for machine-to-machine (M2M) functionality. Fundamentally, the IoT for *mining* allows these 'things' or devices to interact with each other, their environments and the internet, which is then expected to provide a dramatic increase in the uptake of the IoT globally. As a result, it has been stated that the potential scale of the IoT could approach a trillion sensors within the decade (across a multitude of applications encompassing mining and resources exaction plant and the like) [3]. Not only is the sheer potential scale of the IoT worrying, it is the IoT's unique heterogeneity (which may be considered both an advantage and a drawback) which also poses a challenge particularly in relation to cyber-security.

Figure 1 provides a graphical understanding of the relationships between IoT, O/T and M2M and security.

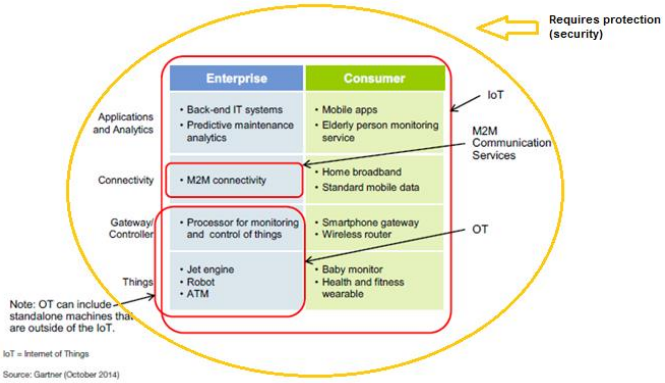


**Figure 1 - Relationship between IoT, O/T, M2M and security [11] (modified by author)**

There exists an emerging, large body of growing evidence, which now highlights the increasing cyber-security awareness in relation to the developing security vulnerabilities currently facing the IoT.

For example, Gartner, the global leader in both IT research and IT advisory, predict that 'by 2017, 30% of threat intelligence services will include vertical-market security intelligence information from the IoT' [7].

Therefore, despite all the IoT advantages, security is the foremost reason put forward for resisting acceptance of this rapidly evolving technology into the mainstream. It is expected that only when these security impediments are addressed, can greater focus be applied to the many other perceived organisational concerns for corporate, business and operational responses to the IoT. Fundamentally, these organisational issues are seen as: the lack of business involvement in IoT security strategy; confusion regarding organisational ownership of IoT; and IoT lacking widely accepted agreements on security standards, specifications, policies, processes, governance, frameworks and guidelines.

This work seeks to address these gaps.

The rest of this paper is organised as follows; the next section presents a sample of the literature review as part of this study, including, IoT standards, security and application in mining. Followed by the proposed methodology and conclusion.

## 2. LITERATURE REVIEW

Many studies have examined the IoT focusing on various parts of the technology and/or its applications. Where some studies have focused on other aspects of IoT, others have specifically examined IoT standards, IoT security, and the IoT with its application for mining.

There do not seem to be any established IoT standards or frameworks tailored for IoT in mining, which have specifically considered aspects such as identity and access control, protocol and network security (i.e. integrity, confidentiality and authentication methods), privacy, trust management, and interoperability, which are all crucial to the IoT's success for mining and resources.

### 2.1 IoT and the OSI model

When understanding the very heterogeneity of the IoT, all 'seven layers (physical, data-link, network, transport, session, presentation, and application layers) of the Open Systems Interconnection reference model (OSI model) have been either discussed emphasised in some way, but rarely has any of the research taken a holistic view of the OSI model when analysing IoT communications in a multifaceted approach.

According to Yu et al. [37], the implementation of secure end-to-end (E2E) communications based on protocols primarily used between internet nodes and sensors can be applied at separate layers of the OSI model; the three main layers for implementing security they found were at the network, transport and application layers. They also found evidence that providing security on the IoT devices themselves was unsuitable due to the sensors themselves lacking the necessary processing power and therefore likened traditional cyber-security countermeasures application to sensors as a denial of service (DoS) attack [37]. Fundamentally, Yu et al. [37] assert that conventional IT security protocols established for the internet usually depend on both symmetric authentication and key management established on public key algorithms. As a result, applying this design philosophy is unsuitable in sensor networks due to the heavily resource constrained nodes themselves. However, Yu et al. [37] did note as part of their study that many standards organisations are presently and vigorously creating standards for the development of sensor network infrastructure.

Alternatively, others scholars like Chen and Lien [5] have taken a different approach when exploring IoT communications and the OSI model. They focused their attention on the physical layer, and they considered other layers too, such as the data link layer, specifically, the Media Access Control (MAC) layer, and the lower sublayer of the data link layer. During their research, Chen and Lien [5] also examined the various wireless infrastructures as per the standards such as Bluetooth (IEEE 802.15.1), Zigbee (IEEE 802.15.4), and WiFi (IEEE 802.11), before finally pursuing 3GPP

(Long Term Evolution - LTE) as the standard for their conceptual model when testing their M2M theories for devices (things). They discovered that, due to the heterogeneous nature of IoT, there exists a number of design issues, and there remains much needed research still to be completed for specifics such like network architecture for both IP wireless LANs and LTE [5].

Research for the IoT has also intensified on the upper layers (transport, session, presentation, application layers) of the OSI model. A number of studies have turned their attention to authentication and access control methods used in the IoT. An example of this was a project delivered by Ndibanje et al. [23].

It was their objective to conduct a thorough review of a previous study by Jing et al. [18]. Specifically, they analysed the method and cryptanalysis of the architecture and authentication process, access control method and session key establishment that the Jing et al. [18] study previously presented. Ndibanje et al. [23] determined that, when evaluating the Jing et al. [18] IoT authentication methods, they found that their proposed protocol 'is vulnerable to compromised device attacks and replay attacks' [23]. Moreover, their results demonstrated that the amended protocol actually placates the requirements of the key security services in the IoT such as 'confidentiality, integrality and authenticity and achieves better efficiency at a lower communication cost' [23].

It becomes clear that an emerging technology such as IoT when devoid of any widely accepted standards can be a challenge. This fact has not gone unnoticed by scholars. The research here seeks therefore to explicitly develop best-practice standardisation guidelines for the mining and resources industry in Western Australia.

## 2.2 IoT standards

A number of studies have found a lack of any widely accepted (and ratified) standards for IoT; the mining industry in WA as a case-in-point. To build towards a mining-specific model, the broader range of industry studies requires discussion.

The study by Qiu et al. [26] found that, with respect to IoT specifically, 'standards are needed to overcome these differences, address the common requirements among diversity sectors, and support a wide range of applications'...and that 'standards are, and will continue, to play an important role both within an organization or entity and across organizations' [26]. This hypothesis was when Qiu et al. [26] were referring to specifically the application of IoT in real-time tracking of assets and their interactions.

Hence, even though the current IoT landscape for standards may be considered undeveloped, this has not inhibited researchers at least examining the process.

The approach taken by Kai et al. [19] attempted to gather data on IoT standards and report the findings on the status of these standards and more importantly, the process to establish them.

Their report titled *Standardising the Internet of Things: What the Experts Think* was aimed at creating preliminary recommendations for developing a process for practitioners and adopters on how IoT standards are set. Ultimately, it was their view that the process for setting today's standards for IoT could be considered adequate; however, they did find that large manufacturers and solution providers, and not industry subject matter experts dominated the process. Also, they found that normal Information Communication Technology (ICT) standardisation does not appear to be even close to being sufficiently represented in the standardisation process concerning the IoT, and the consumer was barely represented in the IoT standards' working groups at all [19].

A lack of any commonly accepted standards for IoT is cause for concern when we consider these technologies in a very safety conscious and engineering standards intensive industry such as mining.

However, it is not only traditional engineering and communication standards for the IoT that are causing angst; specific IoT security standards are also causing concern.

Academics such as Sicari et al. [32] advocate that the 'IoT requires guarantees for security and privacy' [32]. Their study also found that, when considering customary security countermeasures, they appear to struggle when attempting to seamlessly translate across the IT to IoT divide. Their research also highlighted the lack of standards. They provided evidence that this problem is largely due to the dissimilar standards and communication stacks employed by both technologies. Moreover, Sicari et al. [32] also found that, due to the large amounts of interconnected devices in IoT, scalability issues are encountered; and therefore more flexible infrastructure is required to accommodate the security threats in such a dynamic environment.

## 2.3 IoT security

There have been many empirical studies centring their attention on the IoT security. For example, a study by Roman et al. [28] found that one of the major impediments to the widespread adoption of IoT is security concerns [28]. The Roman et al. [28] view is consistent with that of Ashraf and Habaebi [1] who assert that 'Security represents a critical component for enabling the worldwide adoption of IoT technologies and applications' [1].

This notion is also supported by the study undertaken by Qiu et al. [26], who also found that 'security and privacy are two major concerns in building the IoT infrastructure'...and also that 'security of IoT technologies and applications is the key in gaining common acceptance' [26]. Qiu et al.'s [26] findings were also consistent with those of Guo et al. [13] whose study had also previously demonstrated that one of the main impediments for success with IoT is that 'the sharing of data in opportunistic IoT applications can raise significant security concerns, with information being sensitive and vulnerable to privacy attacks' [13].

Security and privacy of the IoT was also examined by Hernández-Ramos et al. [15], they discovered that the latest improvements on pervasive computing and communication technologies, allow a smooth integration of smart devices within the internet, and it also enables a new generation of innovative and useful services for people. However, they also found one main disadvantage to this hypothesis, which was, in order to achieve maximum benefit of these technologically advanced ecosystems, security and privacy

fears needed to be properly confronted. This was the basis for their research titled *SAFIR: Secure Access Framework for IoT-Enabled Services on Smart Buildings*. At the completion of their study they had developed a new security framework to give a universal approach on how to handle security and privacy necessities in IoT situations.

The proposed Hernández-Ramos et al. [15] IoT security framework was based on a three-layered model consisting of a Communications Layer, containing functions such as routing, mobility and gateways. This layer communicates with the Core Components Layer, which encompasses tasks such as management, service, IoT and the security module. The security module comprises additional sub-modules, which are authentication, identity management, authorisation, trust and key management. The final layer of the framework is the Applications Layer. It communicates directly with the Core Components Layer, which facilitates roles such as cloud clients, applications, management interfaces and services.

In direct contrast to the existing current Internet, IoT communication patterns are regularly constructed on short and unpredictable links between objects without a previously recognised trust relationship. Moreover, it is this exact trust issue that the proposed Hernández-Ramos et al. [15] IoT framework comprising main security and privacy components, is expected to overcome.

Elmaghraby and Losavio [9] conducted another study investigating security and privacy concerns. Their project was called *Cyber Security Challenges in Smart Cities: Safety, Security and Privacy*. The main aim of this study was to examine in detail two important aspects of IoT issues, which are related: security and privacy, and ultimately understand their impact on smarter cities. When referring to the term 'cyber-security', Elmaghraby and Losavio [9] consider it the illegal access to information and attacks, which cause disruption to service and availability. They were also concerned about the disappearance of privacy among 'digital citizens' As part of their work, Elmaghraby and Losavio [9] explored privacy protecting systems that collect data and activate an emergency response when required. These are also technological challenges that are interrelated with the present IoT security issues. Another goal of their research was to present a new model which represented the relationship among the person, servers and things, which, according to Elmaghraby and Losavio [9], are major components in smart cities and ones which 'we need to protect'. Because of this project (which had a greater legal emphasis than a technical one), they found that the civil liberties privacy matters concerning data held in IoT devices for smart cities, did not outweigh the benefits that having the IoT brings to those cities.

Although the Elmaghraby and Losavio [9] study did address many IoT security and privacy concerns, their study was limited to smarter cities and neglected other industries like mining or manufacturing.

An example of a study that did focus on the application of IoT security in other industries was Grieco et al.'s [12]. Their research found that security represents the 'cornerstone of the entire IoT-aided robotics world' [12]. The significance of IoT security for functions like robotics, automation and other M2M applications should not be underestimated. Understanding exactly how important IoT cyber-security for M2M communications is further advanced by the work of Chen and Lien [5]. Their study found that M2M communications encompass specific exchanges between both the cyber and physical worlds, which then present a number of different issues in security and privacy.

It is therefore crucial that these IoT security fundamentals specifically, are addressed, when considered in heavily dependent M2M environments like mining, where safety concerns are paramount. What is encouraging is the amount of studies that have been conducted in the area of IoT security specifically, although *research thus far does not appear to have led to the development of many thorough cyber-security frameworks* and/or guidance for adopters and practitioners to follow when executing IoT deployments, *particularly in mining environments*.

## 2.4 IoT and mining

The IoT in mining has enormous benefits particularly with the enhanced management of assets and infrastructure, as per Figure 2.

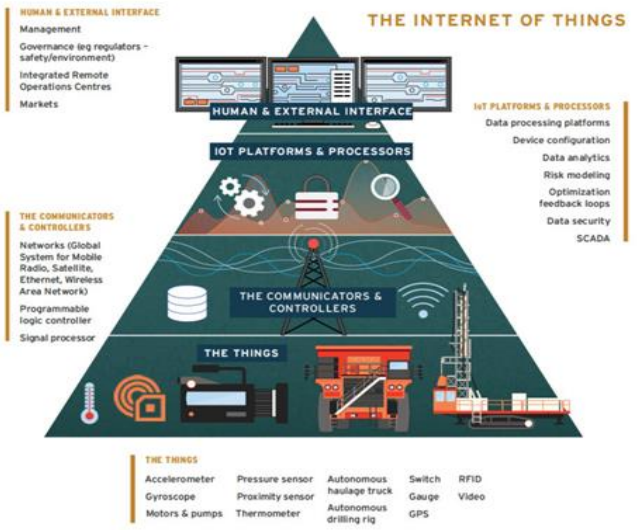


**Figure 2 - IoT for Mining [22]**

Cognisant of the plethora of benefits the IoT may bring to mining, yet focusing on modelling for worker protection, academics such as Yu-fang and Jin-xing [36] evaluated the function of the IoT and the digital mine, with the purpose of improving much needed mine safety in China. Their study, called *Using the Internet of Things Technology: Constructing Digital Mine*, sought to provide a framework for using IoT technology for the construction of a digital mine, and thereby improve designs without risking workers' safety. Understandably, the research was based on the notion that the new IoT technology would eventually be applied to normal mining production practices in Chinese coal mines. Yu-fang and Jin-xing [36] achieved this by developing the digital mine, which was a 'virtual expression' of an actual coalmine. This purely theoretical

mine comprised many complex IT systems in a newly developed framework: multiple platforms, databases, Geographic Information System (GIS) data, production networks (both wired and wireless) the internet, physical sensors and multiple systems for both IT and OT.

Another Chinese research study that concentrated on mining and the IoT was one conducted by Qiuping et al. [27]. The research undertaken by Qiuping et al. [27] undertook an in-depth analysis of all the existing study content associated with mining IoT key technologies and the application of IoT in mines, specifically underground mines. Many of these technologies are required to be IP (Ingress Protection) rated and intrinsically safe due to the ever present risk of disaster caused by floods, fire, gas and dust explosions, cave-ins and the potential for toxic gas releases. The researchers concluded that the technology of IoT application in underground mines can achieve 'precise environment perception and early-warning' for disasters, and the technology can achieve 'precise positioning and automatic identification for underground coal miners and early warning of these disasters' [27].

Further to the previous research, Yinghua et al. [35] continued on the IoT for Chinese mines theme with a study aptly titled *Discussion on Application of IOT Technology in Coal Mine Safety Supervision*. Their objective was to provide a means to use the IoT to aid the coal mining authorities to strengthen the supervision for those enterprises charged with the responsibility for implementing safety in those mines. Their research also analysed the application of the IoT with coalmine safety thoroughly and examined the use of remote sensing technologies. Yinghua et al. [35] showed that, through the adoption of IoT technology, coal-mining safety in China could be given greater priority, specifically with the adoption of the IoT. Which, can therefore be used to track personnel, potentially, illegally moving into restricted or unauthorised areas by the use of a software application that has Radio Frequency Identification (RFID) to define geographical boundaries as a virtual barrier called 'geofencing'. IoT can also enhance emergency response capabilities and accident investigations.

The potential benefits for the application of the IoT in mining could be enormous. Providing connectivity between heterogeneous technologies is an achievement; however, studies point out that it should also be secure. This conundrum has plagued IoT practitioners and their research for some time.

Literature review conducted by this present work shows that certain trends and patterns are starting to appear. A number of the empirical studies have been conducted in the area of IoT security; however limited research attention has been given to studies which offer cyber-security frameworks and/or guidance for adopters and practitioners to follow when executing IoT deployments particularly in mining environments. It would be beneficial to encourage the development of IoT security strategies, policies and frameworks that could give much needed guidance to the mining industry.

Hence, this study aims to thoroughly investigate IoT security practices and then develop a suite of IoT security strategies, policies and frameworks, which will give much needed guidance to the resources industry. Specifically the research proposed here shall seek to examine cyber-security and the IoT by analysing the converged IT/OT with IoT practices and their impacts on mining and infrastructure assets in Western Australia.

The next section aims to provide a tabularised summary of this studies literature review IoT concepts.

## 2.5 Literature review matrix

The IoT literature review matrix in Table 1 represents part of this research that has synthesised particular IoT concepts that are specific to this project.

**Table 1 - IoT Literature Review Matrix**

| Reference | IoT Concepts | | | | |
|---|---|---|---|---|---|
| | IoT Standards | IoT Standards for Mining | IoT Cyber-Security | IoT Security Policies and Frameworks | IoT Security for Mining |
| Ashraf and Habaebi [1] | ✓ | × | ✓ | ✓ | × |
| Bekara [2] | × | × | ✓ | × | × |
| Borges Neto et al. [4] | ✓ | × | × | × | × |
| Chen and Lien [5] | ✓ | × | ✓ | ✓ | × |
| Chen et al. [6] | × | × | × | ½ | × |
| Efremov et al. [8] | ✓ | × | × | × | × |
| Elmaghraby and Losavio [9] | × | × | ✓ | ✓ | × |
| Foell et al. [10] | × | × | × | × | × |
| Grieco et al. [12] | × | × | ✓ | × | × |
| Guo et al. [13] | × | × | ✓ | ½ | × |
| Hawk and Kaushiva [14] | ✓ | × | ✓ | ✓ | × |
| Hernández-Ramos et al. [15] | ✓ | × | ✓ | ✓ | × |
| Herterich et al. [16] | × | × | ✓ | × | × |
| Jamil and Zaki [17] | × | × | ✓ | × | × |

| | | | | | |
|---|---|---|---|---|---|
| Jing et al. [18] | ✗ | ✗ | ✓ | ✗ | ✗ |
| Kai et al. [19] | ✓ | ✗ | ✗ | ✗ | ✗ |
| Lin et al. [20] | ✗ | ✗ | ✓ | ✗ | ✗ |
| Ndibanje et al. [23] | ✗ | ✗ | ✓ | ✗ | ✗ |
| Oh et al. [24] | ✓ | ✗ | ✓ | ✓ | ✗ |
| Qiu et al. [26] | ✓ | ✗ | ✓ | ✓ | ✗ |
| Qiuping et al. [27] | ✗ | ✓ | ✗ | ½ | ½ |
| Roman et al. [28] | ✓ | ✗ | ✓ | ✓ | ✗ |
| Rong et al. [29] | ✓ | ✗ | ✓ | ✓ | ✗ |
| Sanchez et al. [30] | ✓ | ✗ | ✓ | ✗ | ✗ |
| Shin [31] | ✓ | ✗ | ✓ | ✓ | ✗ |
| Sicari et al. [32] | ✓ | ✗ | ✓ | ✓ | ✗ |
| Yang et al. [34] | ✗ | ✗ | ✗ | ✗ | ✗ |
| Yinghua et al. [35] | ✗ | ✓ | ✗ | ✗ | ½ |
| Yu-fang and Jin-xing [36] | ✗ | ✓ | ✗ | ½ | ½ |
| Yu et al. [37] | ✓ | ✗ | ✓ | ✓ | ✗ |

It is evident from the results of Table 1 that a number of studies already undertaken by researchers like Ashraf and Habaebi [1]; Chen and Lien [5]; Hawk and Kaushiva [14]; Hernández-Ramos et al. [16]; Oh et al. [24]; Qiu et al. [26]; Roman et al. [28]; Rong et al. [29]; Shin [31], and Sicari et al. [32] have addressed topics specifically concerning IoT standards, IoT cyber-security and security policies and frameworks in some form.

However, what they have lacked is these specific IoT concepts with their particular development and application to mining in Western Australia.

Identification of the gaps will help this research work toward a resolution of these exact differences.

# 3. METHODOLGY

This research study proposes to evaluate, by way of interview data and document analysis the existing practices and artefacts from selected organisations in Western Australia, where they concern IoT security, moving towards applicability for the localised, WA mining and infrastructure sector.

The study is tapping into the author's extensive contacts across two decades within the industry. It is also targeting 15 very senior expert-practitioners towards data generation stemming from the responses to a list of 40 questions, developed from literature review; and 12 substantive/validated key-areas are developed for the larger sample group of 80-100 (WA mining and resources industry) participants, whom represent major stakeholders in the organisations' IoT, IT/OT convergence and cyber-security decision making and some industry experts. Qualitative analysis is by Statistical Package for the Social Sciences (SPSS). Document analysis complements this work; quantitative data validity of the analysed documents addresses multi-group, non-parametric, uncorrelated statistical analysis tools such as Chi square.

In order to achieve this main aim, a set of specific objectives has been developed:

- Determine the security issues which have arisen with the adoption of the IoT, specifically IT/OT convergence;
- Determine the strategies currently in use for IoT, IT/OT convergence and security;
- Identify operational requirements needed to operate in new IoT and IT/OT environments;
- Determine the current IoT and IT/OT security techniques deployed;
- Identify which standards, specifications, policies and frameworks have been adopted or developed in the case study organisations and how effective they are; and
- Determine the (case-study) organisations' overall IoT, IT/OT convergence and OT cyber-security maturity.

## 3.1 Benefits

It is expected that at the conclusion of this project a number of clear tangible benefits will be recognised, they be;

- A coherent strategy for IoT security to be used for mining;
- A new standard for OT and IoT security, developed specifically for mining, to be considered by resources organisations;
- A logical IoT security policy framework; and
- Comprehensive recommendations for IoT security architectural solution sets, established for the mining industry.

It is probable that the development of these IoT and OT security strategies, policies and frameworks for the WA mining industry will give much needed guidance to the resources industry.

It is also likely that the beneficiaries of this study will range from mining/infrastructure technologies executives to OT engineers and those IT professionals charged with delivering secure outcomes for IoT and IT/OT convergence solutions.

## CONCLUSION

Although this study is currently at its early stages, it has already began to identify gaps in the current research concerning cyber-security for the IoT (namely structural-inadequacies, lack of standards and cyber-security vulnerabilities), with an emphasis on the mining and resources industry in WA. Evidence from a literature review has highlighted that security concerns are real and IoT standards are lacking, together these pose a material threat to mining operations if not addressed or mitigated. This study will once complete, provide tangible guidance on the governance, design and implementation of secure IoT solutions to the industry in Western Australia.

## 4. REFERENCES


[1] Ashraf, Q. M., and M. H. Habaebi. 2015. Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications* 49 (0): 112-127. http://www.sciencedirect.com/science/article/pii/S1084504514002732 (accessed July 12, 2015)

[2] Bekara, C. 2014. Security Issues and Challenges for the IoT-based Smart Grid. *Procedia Computer Science* 34 (0): 532-537. http://www.sciencedirect.com/science/article/pii/S1877050914009193 (accessed March 1, 2015)

[3] Bogue, R. 2014. Towards the trillion sensors market. *Sensor review* 34 (2): pp 137-142. www.emeraldinsight.com/0260-2288.htm (accessed March 17, 2015)

[4] Borges Neto, J., T. Silva, R. Assunção, R. Mini, and A. Loureiro. 2015. Sensing in the Collaborative Internet of Things. *Sensors* 15 (3): 6607. http://www.mdpi.com/1424-8220/15/3/6607 (accessed July 12, 2015)

[5] Chen, K.-C., and S.-Y. Lien. 2014. Machine-to-machine communications: Technologies and challenges. *Ad Hoc Networks* 18 (0): 3-23. http://www.sciencedirect.com/science/article/pii/S1570870513000395 (accessed March 1, 2015)

[6] Chen, S.-L., Y.-Y. Chen, and C. Hsu. 2014. A New Approach to Integrate Internet-of-Things and Software-as-a-Service Model for Logistic Systems: A Case Study. *Sensors* 14 (4): 6144. http://www.mdpi.com/1424-8220/14/4/6144 (accessed July 12, 2015)

[7] Contu, R., S. Deshpande, L. Pingree, E. Ahlm, and C. Lawson. 2015. *Predicts 2015: Security Solutions* http://www.gartner.com/document/2914318?ref=solrAll&refval=170473000&qid=33e9f75496eb2ba7a9ab5b8c5040fb96 (accessed July 11, 2016).

[8] Efremov, S., N. Pilipenko, and L. Voskov. 2015. An Integrated Approach to Common Problems in the Internet of Things. *Procedia Engineering* 100 (0): 1215-1223. http://www.sciencedirect.com/science/article/pii/S1877705815005135 (accessed July 12, 2015)

[9] Elmaghraby, A. S., and M. M. Losavio. 2014. Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research* 5 (4): 491-497. http://www.sciencedirect.com/science/article/pii/S2090123214000290 (accessed March 1, 2015)

[10] Foell, S., G. Kortuem, R. Rawassizadeh, M. Handte, U. Iqbal, and P. Marron. 2014. Micro-Navigation for Urban Bus Passengers: Using the Internet of Things to Improve the Public Transport Experience. http://arxiv.org/abs/1412.6605 (accessed July 22, 2015).

[11] Gartner. 2014. *Relationship between IoT, O/T, M2M and security* http://www.gartner.com/document/2884417 (accessed May 13, 2015).

[12] Grieco, L. A., A. Rizzo, S. Colucci, S. Sicari, G. Piro, D. Di Paola, and G. Boggia. 2014. IoT-aided robotics applications: Technological implications, target domains and open issues. *Computer Communications* 54 (0): 32-47. http://www.sciencedirect.com/science/article/pii/S0140366414002783 (accessed March 1, 2015)

[13] Guo, B., D. Zhang, Z. Wang, Z. Yu, and X. Zhou. 2013. Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things. *Journal of Network and Computer Applications* 36 (6): 1531-1539. http://www.sciencedirect.com/science/article/pii/S1084504513000052 (accessed March 1, 2015)

[14] Hawk, C., and A. Kaushiva. 2014. Cybersecurity and the Smarter Grid. *The Electricity Journal* 27 (8): pp 84-95. http://www.sciencedirect.com/science/article/pii/S1040619014001791 (accessed March 29, 2015)

[15] Hernández-Ramos, J. L., M. V. Moreno, J. B. Bernabé, D. G. Carrillo, and A. F. Skarmeta. 2014. SAFIR: Secure access framework for IoT-enabled services on smart buildings. *Journal of Computer and System Sciences* (0). http://www.sciencedirect.com/science/article/pii/S0022000014001858 (accessed July 17, 2016)

[16] Herterich, M. M., F. Uebernickel, and W. Brenner. 2015. The Impact of Cyber-physical Systems on Industrial Services in Manufacturing. *Procedia CIRP* 30 (0): 323-328. http://www.sciencedirect.com/science/article/pii/S2212827115001924 (accessed July 12, 2015)

[17] Jamil, D., and H. Zaki. 2011. CLOUD COMPUTING SECURITY. *International Journal of Engineering Science and Technology* 3 (4): 3478-3483. ProQuest SciTech Collection. http://search.proquest.com/docview/900364421?accountid=10382 (accessed July 16, 2015)

[18] Jing, L.; Xiao, Y.; Chen, C.L.P. Authentication and Access Control in the Internet of Things. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012; pp. 588–592. (accessed March 4, 2015)

[19] Kai, J., W. Thomas, and R. Kai. 2011. Standardising the Internet of Things: What the Experts Think. *International Journal of IT Standards and Standardization Research (IJITSR)* 1 (9): 63-67. http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/jitsr.2011010104 (accessed July 12, 2015)

[20] Lin, X.-J., L. Sun, and H. Qu. 2015. Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications. *Computers & Security* 48 (0): 142-149. http://www.sciencedirect.com/science/article/pii/S0167404814001229 (accessed July 12, 2015)

[21] Marriott, C. 2015. Into the rusty red. *FinanceAsia*, Feb 2015, 39-41. (accessed July 23, 2016)

[22] Mars. 2014. *IoT for Mining*. http://www.marsdd.com/wp-content/uploads/2014/11/Fig-1-The-IoT-technologies-

in-mining-1-e1415889245363.jpg (accessed May 4, 2015).

[23] Ndibanje, B., H.-J. Lee, and S.-G. Lee. 2014. Security Analysis and Improvements of Authentication and Access Control in the Internet of Things. *Sensors (Basel, Switzerland)* 14 (8): 14786-14805. Pmc. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4179010/ (accessed March 4, 2015)

[24] Oh, D., D. Kim, and W. W. Ro. 2014. A Malicious Pattern Detection Engine for Embedded Security Systems in the Internet of Things. *Sensors (Basel, Switzerland)* 14 (12): 24188-24211. Pmc. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4299106/ (accessed March 4, 2015)

[25] Pettey, C. 2011. Gartner Says the Worlds of IT and Operational Technology Are Converging. *Business Wire*, 2011 Mar 16. ProQuest Central. (accessed March 1, 2015)

[26] Qiu, X., H. Luo, G. Xu, R. Zhong, and G. Q. Huang. 2015. Physical assets and service sharing for IoT-enabled Supply Hub in Industrial Park (SHIP). *International Journal of Production Economics* 159 (0): 4-15. http://www.sciencedirect.com/science/article/pii/S0925527314002795 (accessed March 1, 2015)

[27] Qiuping, W., Z. Shunbing, and D. Chunquan. 2011. Study On Key Technologies Of Internet Of Things Perceiving Mine. *Procedia Engineering* 26 (0): 2326-2333. http://www.sciencedirect.com/science/article/pii/S1877705811052854 (accessed March 1, 2015)

[28] Roman, R., J. Zhou, and J. Lopez. 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* 57 (10): 2266-2279. http://www.sciencedirect.com/science/article/pii/S1389128613000054 (accessed March 4, 2015)

[29] Rong, K., G. Hu, Y. Lin, Y. Shi, and L. Guo. 2015. Understanding business ecosystem using a 6C framework in Internet-of-Things-based sectors. *International Journal of Production Economics* 159 (0): 41-55. http://www.sciencedirect.com/science/article/pii/S0925527314002813 (accessed March 1, 2015)

[30] Sanchez, L., L. Muñoz, J. A. Galache, P. Sotres, J. R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis, and D. Pfisterer. 2014. SmartSantander: IoT experimentation over a smart city testbed. *Computer Networks* 61 (0): 217-238. http://www.sciencedirect.com/science/article/pii/S1389128613004337 (accessed July 12, 2015)

[31] Shin, D. 2014. A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things. *Telematics and Informatics* 31 (4): 519-531. http://www.sciencedirect.com/science/article/pii/S0736585314000185 (accessed July 12, 2015)

[32] Sicari, S., A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks* 76 (0): 146-164. http://www.sciencedirect.com/science/article/pii/S1389128614003971 (accessed March 4, 2015)

[33] WA. 2016. *WESTERN AUSTRALIA ECONOMIC PROFILE – December 2014*. http://www.dsd.wa.gov.au/docs/default-source/default-document-library/wa_economic_profile_1214.pdf?sfvrsn=14 (accessed July 23, 2016).

[34] Yang, L., S. H. Yang, and L. Plotnick. 2013. How the internet of things technology enhances emergency response operations. *Technological Forecasting and Social Change* 80 (9): 1854-1867. http://www.sciencedirect.com/science/article/pii/S0040162512001801 (accessed July 12, 2015)

[35] Yinghua, Z., F. Guanghua, Z. Zhigang, H. Zhian, L. Hongchen, and Y. Jixing. 2012. Discussion on Application of IOT Technology in Coal Mine Safety Supervision. *Procedia Engineering* 43 (0): 233-237. http://www.sciencedirect.com/science/article/pii/S1877705812030512 (accessed March 1, 2015)

[36] Yu-fang, L., and S. Jin-xing. 2011. Using the Internet of Things Technology Constructing Digital Mine. *Procedia Environmental Sciences* 10, Part B (0): 1104-1108. http://www.sciencedirect.com/science/article/pii/S1878029611003719 (accessed March 1, 2015)

[37] Yu, H., J. He, T. Zhang, P. Xiao, and Y. Zhang. 2013. Enabling end-to-end secure communication between wireless sensor networks and the Internet. *World Wide Web* 16 (4): 515-540. http://dx.doi.org/10.1007/s11280-012-0194-0 (accessed March 1, 2015)