2022 IEEE 7th International conference for Convergence in Technology (I2CT)
Pune, India. Apr 07-09, 2022

Analysis of Identity Access Management Controls in IoT Systems

Gerard Ward
Information Systems and Operational Management,
Business School
The University of Auckland
gerard.ward@auckland.ac.nz

Lech Janczewski
Information Systems and Operational Management,
Business School
The University of Auckland
l.janczewski@auckland.ac.nz

2022 IEEE 7th International conference for Convergence in Technology (I2CT) | 978-1-6654-2168-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/I2CT54291.2022.9824010

***Abstract*—The Internet of Things (IoT) describes a computing paradigm in which heterogeneous and connected devices support data-centric processes. Essential in ensuring secure and trustworthy IoT ecosystems, Identity and Access Management (IAM) refers to the policies and technologies used to grant or revoke access to these systems. Following Concept Synthesis of the relevant literature, the directions in IAM technologies are discussed in the context of a preliminary model that can be used to visualize and order extant directions from the literature. This model will help information security practitioners and researchers to visualize and categorize the state of the art in IAM capabilities, necessary to identify how they integrate over an expansive IoT network. In doing so, this will support discussion among the multi-disciplinary experts who may contribute to the modern IoT ensemble. Therefore, this research a) identifies the state of the art in IAM technologies, and b) categorizes the themes specific to IAM in a preliminary model that can help asset owners to maintain continuous representation of IAM capabilities, among other security controls across their IoT assets.**

Keywords—Internet of Things (IoT), Identification Access Management (IAM), reference models, trust.

I INTRODUCTION

The Internet of Things (IoT) describes heterogenous smart devices with embedded sensors and actuators. These computationally capable and tightly coupled devices communicate within networks to support new business models. These new IoT business models are broadly of two types, consumer or industrial. Consumer IoT describes ad-hoc networks that are human-centred, and for which disruption resulting from a loss of data exchange is inconvenient. Industrial IoT describes a machine-orientated architecture supporting real-time Machine-to-Machine (M2M) communication, but for which disruption could result in injury, as well as economic loss.

Consumer applications include healthcare, smart homes, and wearables. Industrial IoT implementations operate within structured networks, with use-cases spanning energy-efficient buildings, preventive maintenance, and smart cities.

However, regardless of the application or use-case, the distributed nature of the IoT creates an enlarged network surface that threat-actors will seek to exploit. Robust network security is required to ensure the volume of data that the industrial IoT system creates in particular, can be processed and stored with semantic integrity [1] in order to maintain system accuracy.

To ensure secure control of the IoT ecosystem's operating state to safeguard data confidentiality, Identity and Access Management (IAM) encompasses the mechanisms used to permit or revoke the right to access, or to update system functions. The access granted by IAM limits the control that a smart device can exercise over those functions to be specific to that device's role within the system. To identify the directions in technologies that can be used to enforce an IoT network owner's IAM policies, this research uses the literature review method known as Concept Synthesis to identify IAM-related thematics from the literature. This is important as the implementation of IAM capabilities reduces the risk of vulnerabilities being exploited by threat-actors seeking unauthorized access to an IoT system. Within IAM, alongside Identity, Authentication into the system, Authorization to access computational resources, and Auditing of activities are referred to as AAA. Today, Cloud services and the software defined services that use them rely on Machine identities for secure non-human M2M communication [2]. IAM therefore needs to address both human and Machine identities, as Machines are a cornerstone of the digital transformations that IoT supports.

To assist the consideration of IoT security, the objective of this research is to create a model that can improve the way that multi-disciplinary parties who contribute to the IoT ecosystem share and discuss security programs, with the example in this research being IAM. Multi-disciplinary experts may be drawn from the often-discrete domains of Information, Operational, and Machine Learning technologies, to support tight system integration at the core of the IoT ecosystem. Also, extensive personal user information may be present, meaning IoT security must account for the financial risks that penalties for failing to safeguard a person's private information give rise to [3].

In this research, section II decomposes the layers that comprise the IoT reference model selected. Section III sets out the research methodology, and section IV presents and discusses the findings derived from extant knowledge in literature. In Section V a representation of the capabilities is visually presented within a generalized IoT reference model. Section VI provides the conclusions of this research.

The next section introduces the adapted IoT Reference Model.

II IOT REFERENCE MODEL

While IoT has been generalized under IoT reference models, many of these focus on the encapsulation and decapsulation of data as a functional representation of the exchange of information between its integrated parts. Therefore, to create a structure for the discussion of IAM technical capabilities, in this research the ITU [4] IoT

Reference Model is extended to frame where extant IAM capabilities sit within a contemporary IoT ecosystem. This is important as NIST notes that security programs must account for "new legislation, directives, or policies" so models must be able to adapt to the "dynamic and flexible nature of information" [3].

As discussed in the Introduction, IoT use-cases are expansive, particularly for industry. Applications for IoT-enabled industrial assets target improving asset optimization, hazard reduction, and automating mundane tasks and roles subject to declining work forces [5]. With the societal gains flowing from the IoT forecast by 2025 set to account for up to US$6.3 trillion in economic benefit [6], realizing projections requires IoT systems to be operably safe and secure. To achieve that, the system must account for the increasing frequency and capability of cyber-attacks and limit the risk of erroneous processes inflicting damage. To improve the evaluation of IAM, this research presents a preliminary model that can assist visualization, categorization, and discussion of data security mechanisms in the IoT. Moreover, this model can accommodate extant IoT knowledge as it emerges, thereby enabling the continuous representation of IoT security capabilities.

To establish a common lexicon that describes IoT integration, a number of reference models have been proposed in the literature. For use in this research, Fig. 1 sets out an adapted four-layer IoT Reference Model as defined by the International Telecommunication Union (ITU) [4]. In Fig. 1, Security Management is extended to include security categories subsequently identified by the IERC [7], including Identity Management, Authorization, and Authentication.

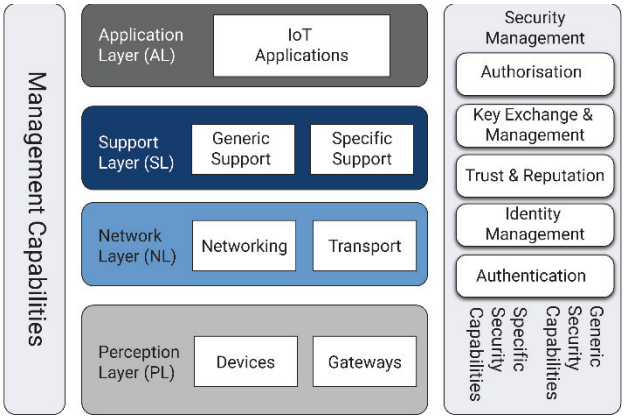

Fig. 1. Extended IoT reference model

Although three-layer IoT systems are common in the literature, a four-layer model enables greater granularity in assessing data flows between integrated systems. Additionally, a four-layer IoT model provides more specificity when mapping its functional layers to the four layers of the Internet protocol suite (TCP/IP), or the conceptual Open Systems Interconnection Model (OSI).

The functional objective of each IoT Layer in Fig.1 is summarized as:

Perception Layer (PL): provides for heterogeneous and tightly coupled sensing and actuating devices that are deployed to measure and physically control the IoT ensemble's operating state. These devices are responsible for the collection of data, which is transmitted to other layers through the NL [8].

Network Layer (NL): interconnects IoT devices with each other, often across the the Internet, using wired and wireless technologies [9]. The NL also supports data flows across the other layers and may use a public-facing network surface such as the Internet.

Service and Support Layer (SL): consists of common capabilities for the storing and processing of data; e.g., Edge, Fog and Cloud computing, SAN, and Data Lakes [9]. Edge and Fog refer to distributed computing with computation closer to the PL to reduce NL data traffic and data latency.

Application Layer (AL): contains the software for the device application, and relies on Session and Presentation layer data as per the OSI data model. The AL uses IT protocols such as Hypertext Transfer protocol (HTTP), and IoT adapted protocols such as Zigbee PRO or CoAP. [10]

In Fig. 1, the panel titled *Security Management* shows *Generic Security Capabilities* and *Specific Security Capabilities*. Generic refers to those that are not discrete technologies, services, or products, and are thus independent of applications [11]. IAM is a generic capability. Specific capabilities are closely coupled with applications to facilitate application-level security across the highly integrated IoT ecosystem [11]. This research focuses on the IAM thematics appropriate to the generic capabilities required to support geographically distributed IoT ecosystems.

To aid real-world contextual understandings, [12] notes that preliminary models can be used to refine functional feasibility in subsequent research to improve utility. Consequently, the main contributions of this paper are: i) an up-to-date mapping of the state of the art in the context of IoT IAM, and ii) a preliminary model to describe information security trends specific to the IoT. The audience targeted by this research and the result artefact is composed of: i) information security and risk management practitioners who need to consider both current and future IAM protections, and ii) researchers who are aiming to map and update their baseline that measures the directions in the IoT.

The next section sets out how the Concept Synthesis of the themes identified from relevant IoT literature was progressed.

III METHODOLOGY

To synthesize concepts from the literature the methods used by were adapted from the field of Semantic Reduction (SR) and Corpus Linguistics (CL) [5]. SR is a textual summarization process where words that do not contribute to the pool of literature being analyzed are deleted from the body of text. CL is a quantitative method of language analysis used to examine the frequency of words and phrases in a domain-specific corpus to assist the identification of prevalent themes. The use of the SRCL method approximates the objectives of PRISMA 2020, a research reporting method that specifies a systematic approach for synthesizing concepts from literature and medical studies [13].

In this research, the literature analyzed is the IoT corpus created following SRCL reduction. The papers synthesized to create the corpus were drawn from IEEE and Elsevier databases in 2021. The process steps were:

Selection of peer-reviewed literature: A total of 3,040 papers published in 2021 (excluding 591 duplicate papers) were selected for review from IEEE and Elsevier ScienceDirect (SD) databases using Boolean search criteria. The search terms applied were: *Internet of Things*, or *Industrial IoT*, or *I4.0*, or *Industry 4.0*, or *Industrie 4.0*, as well as *risk management*. Including the term Industrial IoT (IIoT) ensured that considerations related to industrial Internet-enabled M2M communications were captured. Equally, the value creation processes Industry 4.0, Industrie 4.0, and I4.0, were included. These terms refer to the innovations in manufacturing that leverage IoT technologies. Risk management was used to capture themes related to risk and IAM controls.

Screened: 577 papers were drawn from IEEE, and 1,872 from SD (Decision Sciences 274, Computer Science 775, Engineering 823). A further 491 papers downloaded from SD were found to be duplicates across the three SD categories.

Papers were semantically reduced: A semantic reduction tool developed in Python [5] was used to remove text such as pronouns and other non-relevant terms, which reduced the total word count by 13,145,360 words, or 46%.

Metadata analysis of the corpus: The 2,449 conditioned articles were uploaded to a metadata analysis tool for examination as a single corpus [14].

Themes in the resulting corpus, once identified, were analysed in iterative cycles, with the findings set out in the following section. The authors independently reviewed and identified themes, which were then compared and discussed prior to inclusion in this research. If required, themes identified were supplemented with further content using Google Scholar. In the next section, the considerations and state-of-the-art directions covering IAM present in the IoT corpus are discussed. Where themes specific to one of the 2,449 papers in the corpus are directly referenced, that work is cited accordingly.

IV IAM, The State-of-the-Art

Extant knowledge is set out in this section against the IoT Layers presented in Fig. 1.

A. Perception Layer (PL)

Across the 2,449 papers synthesized, 38 papers referenced the PL. Before discussing the specifics of Identify, to frame the general characteristic of smart IoT devices in a contemporary IoT implementation, is that they are likely to be computationally capable Micro Controller Units (MCU) [15]. These smart devices may include: a Central Processor Unit (CPU), memory, sensors and actuators, and are Internet enabled [16]. The MCU can complete complex computation through the incorporation of a Real Time Operating System (RTOS), which mimics the multi-thread multi-task functionality of more complex CPUs [17]. Inbuilt input and output (I/O) interfaces provide for the signal conversion of external sensors and actuators.

To account for integration and connectivity across the computational powerful devices and the IoT Layers, Fig. 2 shows the dominant collocated concepts when mapping the anchor terms '*IAM*' and '*Data Networks*'. Collocated concepts measure word frequency within a defined span [14] with Fig. 2 illustrating the relationship between the anchor terms and other concepts from within the corpus. Where the *Themes* and *Collocates* drawn from Fig. 2 are explored in this Section, reference to those terms is *italicized*.

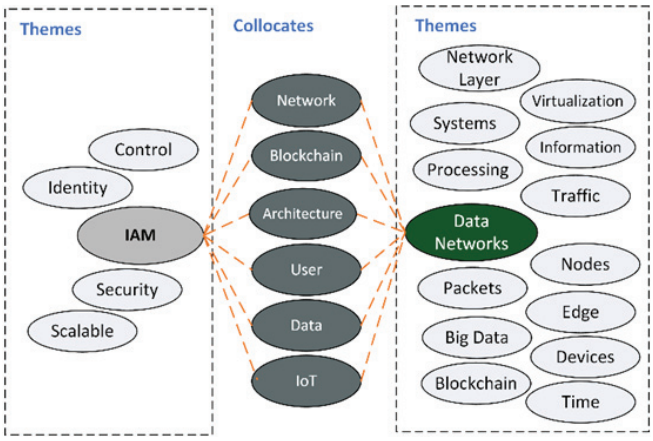

Fig. 2. Collocated themes between IAM and NL

Extant considerations relevant to IAM in the PL are discussed in the following Subsubsections.

Identity: For initial *Device* introduction into the ecosystem, Physical Unclonable Functions (PUFs) [18] that are unique to the MCU can be used to confirm *Identity*. Robust PUF mechanisms designed to prevent device cloning include non-linear, unique chip identifiers inserted during manufacture, with reliability rates of 75% to 95% [18]. However, the complexity and cost of implementing these PUF fingerprints is significant [18]. Alternatively, the IETF has recently proposed using the Manufacturer Usage Description (MUD), whereby Machine Learning rules and a strictly defined role-based access policy limit variation or escalation of processes beyond those permitted [8]. To support trust in device re-authentication (a requirement of AAA), complex PUFs can use a bit-string challenge/response, to uniquely identify each device [18].

In Fig. 2, *Time* is shown to be a prevalent theme in IoT systems, particularly those that exercise physical control over a process. Therefore, the system requires an awareness of time and space, bound by feedback loops [19]. In operational use-cases, the introduction of rogue IoT *Devices* into time-sensitive environments may risk physical damage if the accuracy of measuring *Time* and space is maliciously altered.

Device Provenance and COTS: The literature discusses instances where an attacker can assume the identity of an authenticated user. Examples of this class of physical attack include potentially tampering within the CPU through the device's JTAG interface [8]. If successful, the hardware circuitry can be altered [20]. Additionally, highlighting supply chain risk, fault-injection attacks, and physical and architectural vulnerabilities could be introduced into the design and manufacturing processes [21]. The literature identifies that current manufacturing processes are not equipped to detect anomalies, or implement countermeasures, making detection of such attacks challenging [21].

In the absence of formal quality verification, there is risk in untested Commercial Off The Shelf (COTS) *Devices*, which may not be subject to security evaluation. Adding to the complexity, connecting disparate COTS IoT *Devices* to access points creates risk because of potential variability in security policies within that ecosystem exacerbating identity

risk. IERC [22] notes that this is of particular concern in IoTs, where variability in design processes may "create new vulnerabilities as integration issues may arise".

Self- awareness: For smart devices with RTOS installed, Neural Network (NN)-type algorithms are capable of regulating system performance and correctness. In previous studies, as a *Security* measure self-healing architectures installed on MCUs with RTOS installed have been used to repair the system when malicious faults are encountered [10].

Blockchain: Fig. 2 shows that that a prevalent theme in IAM and IoT is the use of the *Blockchain* to address single points of failure in hierarchical authentication systems [23]. For example, [24] proposes using *Blockchain* to maintain device identities in an immutable distributed ledger [25]. To address *Device* identification and authentication as well as security in an open data exchange, [26] proposes a *Blockchain* model with 60% reduction in computation, storage and communication costs, compared to other Blockchains.

While in Fig. 1, *Gateways* in the PL are presented as being at the PL, given the trend away from hardware or physical gateways since the IoT reference model was published in 2014 [4], Software Defined Networks (SDNs) have become increasingly common as per the thematics *Network Layer* and *Virtualization* in Fig. 2. Therefore, SDNs are discussed in the next section [27] addressing the NL. Also, M2M communication will be orchestrated over well-specified gateways [28].

B. Network Layer Risk (NL)

The NL encompasses the network and communication functions including communication protocol routing and addressing, the quality of network services (QoS), and protocol flow control for error correction and reliability [7]. Additionally, the NL integrates the PL with higher-level software and data storage. Therefore, the NL coordinates the authentication and management of every endpoint within the ecosystem [29].

Threats within the NL that impact IAM have been discussed in 95 papers, ranging from data *packet* interception using Man-in-the-Middle attacks (MITM), to exploitation of TCP/IP and its lightweight variant the User Datagram Protocol (UDP) [30]. Additionally, the Domain Name System (DNS), which maps domain names to IP addresses, can be exploited [30]. While TCP/IP has become the default client/server communications protocol for the Internet, is designed to support cost effective data routing, it lacks explicit security [31]. Consequently TCP/IP relies on external architectures to address vulnerabilities, particularly at the NL interlayer [32].

Traditionally, network *traffic* was managed in a hardware-centric manner, using dedicated hardware devices such as routers and switches. Changing that paradigm, SDNs have moved the data control plane from decentralized hardware to software [33]. The use of SDNs is referenced in 96 of the papers synthesized. While SDNs are considered to support network resiliency, security challenges relevant to IAM include increased complexity in terms of authentication and authorization schemes [34]. Architectural constraints include limited memory for flow rule storage, and controllers can become a single point of failure, with distributed controllers requiring focus on authentication, consistency, and scalability (*Scalable*) [34]. Additionally, saturation attacks, Distributed Denial-of-Service (DDoS) attacks, and MITM attacks can also be deployed against SDNs [34]. In terms of system attacks, a very prevalent threat discussed is DDoS. As a DDoS exhausts ecosystem resources, it can slow or prevent authentication onto the IoT network or limit the resource availability necessary to support the bi-directional vertical data flows implicit in Fig. 1. The move towards SDNs in the IoT may also assist the application of Zero-Trust segmentation frameworks premised on the assumption that a complex network's security is subject to continual external and internal threats.

Other literature [28] notes that integrated network intrusion detection is necessary across the PL, NL, and SL, alongside robust AAA practices to address SDNs and IAM shortcomings. Also, the *Blockchain's* use in support of auditing (the third A in AAA) is unsurprising, given its prevalence in the literature as shown in the themes presented in Fig. 2. In the supply chain, [35] discusses auditing processes enhanced with immutable records.

C. Service and Support Layer (SL)

As discrete terms, the Support Layer is referenced in only 5, and the Service Layer in 37 of the papers synthesized. In this research, the terms are used interchangeably and denoted as SL. The SL consists of common ensemble capabilities responsible for storing and processing mass data, such as the *Node* implementations *Edge*, Fog, Cloud, Data Lakes and data analytics, which will also be necessary to support Industrial IoT. Cloud and Data Lakes in particular support *Big Data* analytics to bring greater fidelity to the operation of the IoT business models discussed in the Introduction. Also, this *Information* fidelity will support great system autonomy, with the extent of *Control* in industrial applications limited by the extent of hazard system failings present [36].

Within the SL Layer an emergent trend is software-defined services termed Microservice Architecture (MSA), for use in cloud applications [1]. MSA describes technology that many application development teams are employing, involving small independent services that communicate over well-specified Application Programming Interfaces (API) [28]. Security evaluation of these containerized MSA applications involves static code review, privilege and permission control within the IAM framework, and complete logging of all updates and execution [37]. Alongside usernames and passwords for human identification and authentication, the digital identities of Machines rely on cryptographic keys and digital certificates [37]. Robust IAM practices are vital where Machines control autonomous decisioning, which threat actors could manipulate to create an unsafe operating state.

Threats identified in the literature include DDoS attacks, malicious insiders, and unauthorised access, with controls including secret keys and passwords [38]. By comparison, AAA is referenced across 19 texts. While directions in the literature include the use of Access Control Lists (ACL) protected by the *Blockchain*, a centralised administrator must be responsible for the addition and revocation of entities in an industrial setting [39]. It is the compromise of privileged credentials, and lateral movement across networks, that is a characteristic of many current IT-type attacks [40]. SL-specific policies must incorporate robust security policies, designed to thwart attacks of this class.

Many of these services may be consumed as on-demand computing resources, accessed by users over the Internet, and typically operated by third parties [41]. These providers may use multi-tenancy architectures to multiplex the execution of multiple client Virtual Machines (VM) [42]. *Virtualization* was shown as being a prominent network-related theme in Fig. 2. In Platform-as-a-Service (PaaS) Cloud models, the presence of malware in a single VM could threaten other VMs that coexist on the same computing surface [42]. While virtualized and containerized architectures could provide controls, the provisioning and monitoring of countermeasures may be the responsibility of the Cloud service provider. If failure occurs, access by the data owner to data forensic *information*, for use in root cause analysis, may be limited.

Highlighting multidimensional risk, virtualized containers in increasingly software-defined deployments, isolated by namespaces, share the OS kernel. Kernel-level rootkit exploit vulnerabilities may lead to the namespace being invalidated, by granting the server within the container permission to view, or even affect other containers [43]. Kernel-level exploits effectively grant access to the shared network. In Microsoft Windows domain-based IT systems, some namespace configurations depend on an Active Directory (AD). However, credential harvesting from an AD is a common technique that threat actors use to escalate privilege within IT networks [44].

This reliance on third-party Cloud and Data Lakes may shift the technical risk to a third party. Normally, third-party performance would be addressed under mutually agreed contracts. However, the concentration of market power in large Cloud providers means Service Level Agreements (SLAs) are often not well defined, and may have significant variance across QoS, security policies, and governance [45].

D. *Application Layer (AL)*

The AL consists of software applications. Attacks and vulnerabilities referenced in 131 papers synthesized include threats and vulnerabilities specific to the control plane, channel, and data plane, including weak authentication and authorization.

Literature referencing the AL is varied, with topics canvased ranging from, and reflecting, multi-dimensional risk such as identity resolution [23] as discussed in PL. Traditional IT systems and the AL share similar functionality and therefore, may be presented with the same class of vulnerabilities and threats; e.g., SQL injections and DDoS [30]. Within the AL the general themes regarding security capabilities include the use of VMs and containerization, as well as applications being installed over SDNs as independent data consumers [46].

E. *Other Themes – Trust & Reputation*

In section II, Fig. 1 introduced the objectives of IAM necessary to ensure *Trust & Reputation* across the IoT ecosystem, and integrity in the processes that IoT data supports.

NIST defines trust as a "characteristic of an entity that indicates its ability to perform certain functions or services correctly…along with assurance that the entity and its identifier are genuine" [47]. Trust and reputation are issues directly relevant to COTS authenticated into the PL, as well as the third-party-provided services of *Edge*, Fog, Cloud, and Data-Lakes. At the time of connection, Machines check keys and certificates to establish trust, to authenticate other Machines, and for use in encrypting communications.

Therefore, reputation is necessary in the appraisal of third party vendors where the enlarged IoT network surface needs to now account for supply chain risk, and where scope for contractual certainty may be limited [5].

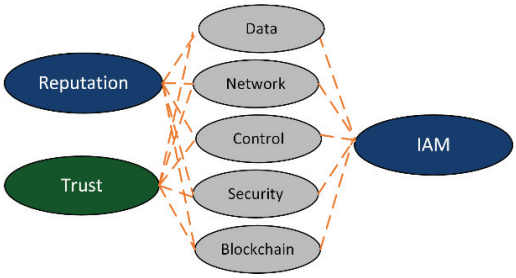

Fig. 3. Prevalence of Blockchain in trust and reputation

While the collocated themes shown in Fig. 3 between reputation, trust and access management of data, network, control, and security are unsurprising, they illustrate the prevalence of Blockchain as a topic in the literature. Its use in IoT is discussed in multiple use-cases. For example, in IAM it is conceptually demonstrated as supporting authentication and therefore verification of Cloud-hosted data, using intelligent algorithms to create immutable data records derived from PL smart devices [27].

V PRELIMINARY IOT MODEL

The IERC [48] notes that the IoT involves multidisciplinary activities with different meanings "at different levels of abstraction". To help bring structure and perspective to the IoT abstraction, as well as the IAM thematics discussed in the previous Section, Fig. 4 summarizes these findings in a novel IoT preliminary model.

The yellow rectangles in Fig. 4 show the technologies supporting IAM generic capabilities. Many considerations are shown to be present across multiple layers.

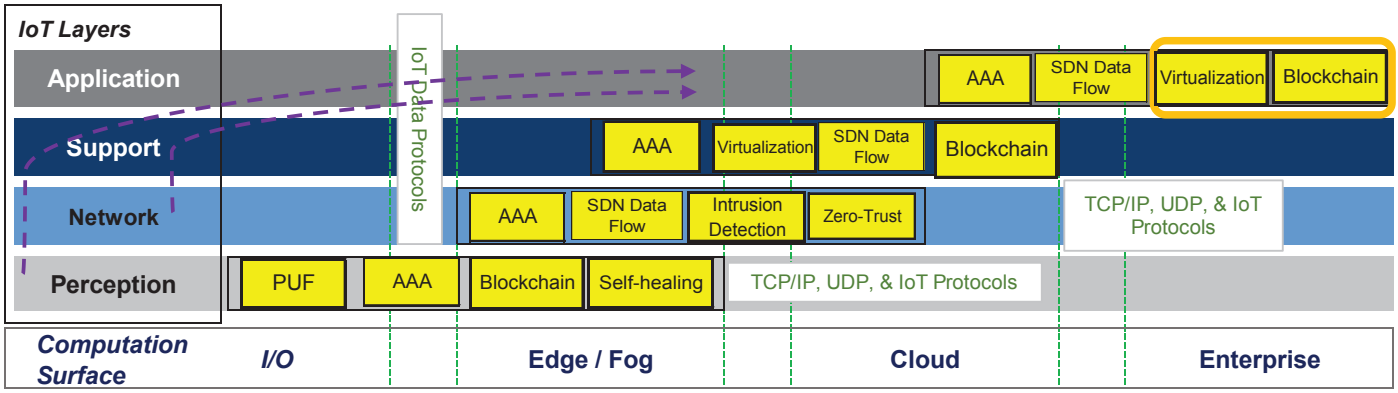

Fig. 4. IoT generalized model

For example, as AAA is a core requirement of trustworthy distributed processing, the Generic Security Capabilities of authentication and authorization are required at all points of intersection between the IoT Layers and the Computational Surface (CS). This is necessary to prevent rogue devices and users being introduced, as well as unnecessary access to resources.

In Fig. 4, the horizontal section labelled as the Computation Surface (CS) represents the distributed computational architectures present in contemporary IoT ecosystems. Even when provided as a cloud service, for the storage and processing of data, the architectures of the CS are hardware centric. Smart devices in the PL are labelled I/O to account for signal processing.

The IoT Layers in Fig. 4 are the same as those presented in Fig.1. Differentiating the IoT Layers from the CS are the layers supporting the bi-directional data flows necessary to integrate the systems functions that inform IoT processes. Data communication emanating from the PL and I/O layer relies predominantly on IoT protocols, with TCP/IP, UDP, or IoT-adapted TCP protocols supporting enterprise-level Application Layer functions. The green dashed lines show the vertical movement of data up the IoT Layers. Data will also move across these boundaries to other computation states within the CS. The orange border represents Data Lakes, the Cloud model used for mass storage of raw IoT-derived data that supports greatly system fidelity.

In Fig. 4, the purple lines illustrate that the traditional boundaries, which characterize process and automation hierarchies [49], and that may be less rigid in contemporary IoT system when compared to legacy industrial systems (subject to the extent of hazard). Internet-connected devices in the PL can push data direct to the AL Data Lakes. Therefore, use of the model can also aid the evaluation of emergent Zero-Trust capabilities, where segmented zones rather than perimeters are created to enforce data confidentiality and integrity [50].

Thus, the instantiation in Fig. 4 presents a preliminary model that can be used to baseline the current knowledge in IoT. This can assist determination of where emergent security functions could contribute to robust IoT system security, including IAM.

VI Conclusions, Future Research

This research presents an analysis of the state of the art related to the IoT IAM. The findings as presented in the generalized model shown in Fig. 4 frame the multi-dimensional nature of security management capabilities necessary to ensure secure trustworthy IoT systems.

Concept Synthesis was completed following the use of SRCL to create an IoT-related corpus from the selected literature. This analysis was guided by the disciplines of PRISMA to bring structure to the process, and can assist the continuous representation of security capabilities by identifying incrementally new security themes as they emerge.

The purpose of the model presented in Fig. 4 is to provide a means by which the multi-dimensional requirements of generic security capabilities can be visualized. The intention is to support multi-disciplinary expert discussion around IoT security considerations, particularly risk that may be present when generic security capabilities such as IAM are not provisioned correctly over the enlarged network surface the IoT creates.

Additionally, it provides a model in which the role of emergent themes such as those discussed in Section IV can be considered in the context of the IoT ecosystem. The development of this preliminary model aligns with Information Systems research [12] where rudimentary prototypes are used to test functional feasibility. Therefore, this preliminary model will be subject to future expert refinement to inform proof-of-value and use. That will progress the objective of developing a systematic design for evaluating extant knowledge around IAM controls in the IoT. This will assist the evaluation of safe and secure IoT processes, while optimizing the availability of process-critical data that IoT-dependent business models rely upon. Equally, the model will be sufficiently generalized for use in evaluating other emergent practices or technologies in the IoT.

I. References

[1] G. Campeanu, "A mapping study on microservice architectures of Internet of Things and cloud computing solutions," in 2018 7th Mediterranean Conference on Embedded Computing (MECO), 10-14 June 2018 2018, pp. 1-4, doi: 10.1109/MECO.2018.8406008.

[2] Venafi, TLS Machine Identity Management. New York: Wiley, 2021.

[3] NIST, "Managing Information Security Risk," in "Special Publication 800-39," Maryland, 2011, vol. SP 800-39.

[4] ITU, "Overview of the Internet of things," in "Telecommunication Standardization Sector," International Telecommunication Union, Geneva, 2012, vol. ITU-T Y.2060. [Online]. Available: www.itu.int

[5] G. Ward and L. Janczewski, "Using Knowledge Synthesis to Identify Multi-dimensional Risk Factors in IoT Assets," in Third International Conference on Advances in Cyber Security, Singapore, 2021: Springer, in Advances in Cyber Security, pp. 176-197, doi: 10.1007/978-981-16-8059-5_11.

[6] M. Chui, M. Collins, and M. Patel, "The Internet of Things: Catching up to an accelerating opportunity," McKinsey & Company, November 2021 2021. [Online]. Available: www.mckinsey.com.

[7] D. Darwish, "Improved layered architecture for Internet of Things," International Journal of Computing Academic Research (IJCAR), vol. 4, no. 4, pp. 214-223, 2015.

[8] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and Opportunities in Securing the Industrial Internet of Things," IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 2985-2996, 2021, doi: 10.1109/TII.2020.3023507.

[9] L. Xing, "Reliability in Internet of Things: Current Status and Future Perspectives," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6704-6721, 2020, doi: 10.1109/JIOT.2020.2993216.

[10] E. Pricop, J. Fattahi, N. Dutta, and M. Ibrahim, Recent developments on industrial control systems resilience. Switzerland: Springer, 2020.

[11] M. Muckin and S. C. Fitch, "A threat-driven approach to cyber security," Lockheed Martin Corporation, 2014.

[12] J. F. Nunamaker Jr, R. O. Briggs, D. C. Derrick, and G. Schwabe, "The last research mile: Achieving both rigor and relevance in information systems research," Journal of management information systems, vol. 32, no. 3, pp. 10-47, 2015.

[13] A. C. Tricco, E. Lillie, W. Zarin, K. K. O'Brien, H. Colquhoun, and D. Levac, "Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation," Annals of Internal Medicine, vol. 169, no. 7, pp. 467-473, 2018, doi: 10.7326/m18-0850.

[14] V. Brezina, M. Timperley, and A. McEnery, "#LancsBox v6.0 Manual," Lancaster University, UK, 2021. [Online]. Available: corpora.lancs.ac.uk/lancsbox/help.php

[15] M. Bates, "PIC Hardware," in PIC Microcontrollers M. Bates Ed., Third Edition ed. Oxford: Newnes, 2014, pp. 93-106.

[16] E. A. Lee and S. A. Seshia, Introduction to Embedded Systems : A Cyber-Physical Systems Approach, Second Edition, Version 2.2 ed. Massachusetts: MIT Press, 2017.

[17] M. A. Sehr, M. Lohstroh, M. Weber, I. Ugalde, M. Witte, and J. Neidig, "Programmable Logic Controllers in the Context of Industry 4.0," IEEE Transactions on Industrial Informatics, 2020.

[18] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A taxonomy of PUF Schemes with a novel Arbiter-based PUF resisting machine learning attacks," Computer Networks, vol. 194, p. 108133, 2021, doi: 10.1016/j.comnet.2021.108133.

[19] A. Bécue, I. Praça, and J. Gama, "Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities," Artificial Intelligence Review, vol. 54, no. 5, pp. 3849-3886, 2021, doi: 10.1007/s10462-020-09942-2.

[20] M. Snehi and A. Bhandari, "Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks," Computer Science Review, vol. 40, p. 100371, 2021, doi: 10.1016/j.cosrev.2021.100371.

[21] H. Wang, H. Li, F. Rahman, M. M. Tehranipoor, and F. Farahmandi, "SoFI: Security Property-Driven Vulnerability Assessments of ICs Against Fault-Injection Attacks," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, pp. 1-1, 2021, doi: 10.1109/TCAD.2021.3063998.

[22] IERC, "IoT Governance, Privacy and Security Issues," in "European Research Cluster on the Internet of Things," IoT European Research Cluster, Oslo, 2015. [Online]. Available: www.internet-of-things-research.eu

[23] Y. Ren, R. Xie, F. R. Yu, T. Huang, and Y. Liu, "Potential Identity Resolution Systems for the Industrial Internet of Things: A Survey," IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 391-430, 2021, doi: 10.1109/COMST.2020.3045136.

[24] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski, "The Security Reference Architecture for Blockchains," IEEE Communications Surveys & Tutorials, vol. 23, pp. 341-390, 2021, doi: 10.1109/COMST.2020.3033665.

[25] IIC, "Industrial Internet of Things Volume G4: Security Framework," Industrial Internet Consortium, Massachusetts, 2016, vol. IIC:PUB:G4:V1.0:PB:20160926. [Online]. Available: iiconsortium.org

[26] L. Vishwakarma and D. Das, "SCAB - IoTA: Secure communication and authentication for IoT applications using blockchain," Journal of Parallel and Distributed Computing, vol. 154, pp. 94-105, 2021, doi: 10.1016/j.jpdc.2021.04.003.

[27] Z. Eghbali and M. Z. Lighvan, "A hierarchical approach for accelerating IoT data management process based on SDN principles," Journal of Network and Computer Applications, vol. 181, p. 103027, 2021, doi: 10.1016/j.jnca.2021.103027.

[28] P. P. Ray and N. Kumar, "SDN/NFV architectures for edge-cloud oriented IoT: A systematic review," Computer Communications, vol. 169, pp. 129-153, 2021, doi: 10.1016/j.comcom.2021.01.018.

[29] A. Gilchrist, The Industrial Internet of Things. Berkeley: Springer, 2016.

[30] N. Magaia, R. Fonseca, K. Muhammad, A. H. F. N. Segundo, A. V. L. Neto, and V. H. C. d. Albuquerque, "Industrial Internet-of-Things Security Enhanced With Deep Learning Approaches for Smart Cities," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6393-6405, 2021, doi: 10.1109/JIOT.2020.3042174.

[31] M. Shah, V. Soni, H. Shah, and M. Desai, "TCP/IP network protocols — Security threats, flaws and defense methods," in 3rd International Conference on Computing for Sustainable Global Development, 16-18 March 2016 2016, pp. 2693-2699.

[32] T. Stergiou, M. S. Leeson, and R. J. Green, "An alternative architectural framework to the OSI security model," Computers & Security, Article vol. 23, pp. 137-153, 1/1/2004 2004, doi: 10.1016/j.cose.2003.09.001.

[33] W. Odom, CCNA 200-301 Official Cert Guide. New Jesery: Cisco Press, 2019.

[34] I. A. Valdovinos, J. A. Pérez-Díaz, K.-K. R. Choo, and J. F. Botero, "Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions," Journal of Network and Computer Applications, vol. 187, p. 103093, 2021, doi: 10.1016/j.jnca.2021.103093.

[35] M. Asante, G. Epiphaniou, C. Maple, H. Al-Khateeb, M. Bottarelli, and K. Z. Ghafoor, "Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey," IEEE Transactions on Engineering Management, pp. 1-27, 2021, doi: 10.1109/TEM.2021.3053655.

[36] ISA. "Industrial Automation and Control System Taxonomy." gca.isa.org (accessed 3 October 2021.

[37] SANS, "Practical Guide to Security in the AWS Cloud," 2020. [Online]. Available: https://pages.awscloud.com/awsmp-book-SEC-SANS-Practical-Guide-Security-AWS-Cloud.html.

[38] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T. H. Kim, "A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review," IEEE Access, vol. 9, pp. 25344-25359, 2021, doi: 10.1109/ACCESS.2021.3057766.

[39] D. Wu and N. Ansari, "A Trust-Evaluation-Enhanced Blockchain-Secured Industrial IoT System," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5510-5517, 2021, doi: 10.1109/JIOT.2020.3030689.

[40] OWASP. "OWASP Internet of Things (IoT) Project." https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project (accessed 18 August 2021.

[41] L. Thames and D. Schaefer, Cybersecurity for industry 4.0. Springer, 2017.

[42] S. A. Hussain, M. Fatima, A. Saeed, I. Raza, and R. K. Shahzad, "Multilevel classification of security concerns in cloud computing," Applied Computing and Informatics, 2015, doi: 10.1016/j.aci.2016.03.001.

[43] W. Lee and M. Nadim, "Kernel-Level Rootkits Features to Train Learning Models Against Namespace Attacks on Containers," in 2020 7th IEEE International Conference on Cyber Security and Cloud Computing, 2020, pp. 50-55, doi: 10.1109/CSCloud-EdgeCom49738.2020.00018.

[44] Microsoft, "Microsoft Digital Defense Report | September 2020 " 2020. [Online]. Available: www.microsoft.com.

[45] Z. Mahmood, Fog Computing: Concepts, Frameworks and Technologies. Switzerland: Springer, 2018.

[46] J. C. Correa Chica, J. C. Imbachi, and J. F. Botero Vega, "Security in SDN: A comprehensive survey," Journal of Network and Computer Applications, vol. 159, p. 102595, 2020.

[47] E. Barker, M. Smid, and D. Branstad, "A Profile for U.S. Federal Cryptographic Key Management Systems," in "SP800-152," NIST, Maryland, 2015.

[48] IERC, "The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge," in "IERC Cluster SRIA 2018," IoT European Research Cluster, Oslo, 2018.

[49] O. Vermesan and P. Friess, Internet of Things – From Research and Innovation to Market Deployment. Denmark: River, 2014.

[50] M. J. Haber, Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations, 2nd ed. Berkeley: Apress, 2020, pp. 295-304.