A Survey on Unified Modeling under Identification Exploding Tendency in the Internet of Things

Shiquan Dong, Zhou Fang*, Zhimin Zhang, Fadi Farha, Huansheng Ning
University of Science and Technology in Beijing, 100083, Beijing, China
Email: shiquandong@xs.ustb.edu.cn, zhoufang@ies.ustb.edu.cn, zhangzhimin@xs.ustb.edu.cn,
fadi_farha@yahoo.com, ninghuansheng@ustb.edu.cn

2021 International Wireless Communications and Mobile Computing (IWCMC) | 978-1-7281-8616-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/IWCMC51323.2021.9498832

***Abstract*—The prevalence and large-scale uptake of the Internet of Things (IoT) have led to a growing trend of Identification Exploding, namely heterogeneous entities respectively identified to provide convenient intelligent services. To address challenges under Identification Exploding, unified modeling has become a promising approach to generalizing identification for heterogeneous entities in IoT. This paper surveys and discusses Identification Exploding's background to explore the possibility of unified modeling as one of the solutions. Meanwhile, challenges of realizing unified modeling are discussed. After that, comprehensive reviews on the latest modeling approaches and methods covering various IoT entities are carried out, including sensed entities and sensing devices. Special attention has been paid to modeling under resource-constrained IoT environments and relevant modeling-based industry solutions with critical analysis. It is proved that unified modeling is extremely significant under Identification Exploding Tendency in the IoT era.**

***Index Terms*—Internet of Things (IoT), Identification Exploding, Unified Modeling.**

I. Introduction

20 years have passed since Kevin Ashton introduced the concept of the Internet of Things (IoT), identifying interoperated objects with Radio Frequency Identification (RFID) in the supply chain. The IoT now permeates our daily lives, sensing billions of entities with access to the cloud, and providing pervasive services for users all over the world. Between 2016 and 2030, the number of IoT connected devices worldwide are expected to reach nearly 20 billion [1] with around 6 billion Internet users [2]. Ubiquitous entities waiting to be identified are flooding into cyberspace, dubbed as "Identification Exploding".

In Leibniz' Law, identity was defined in the notation of symbolic logic: $\forall F(Fx \leftrightarrow Fy) \rightarrow x = y$. If and only if entity y has the same attributes F of entity x, then x is identical to y. This formulation of the principle reveals that the essence of identification is the mapping of entities' specific attributes. Following this, ITU defined conceptions related to identity in ISO/IEC 24760-1:2011 and updated in ISO/IEC 24760-1:2019, where identification refers to the "process of recognizing an entity in a particular domain as distinct from other entities", and entity refers to the "item relevant for the purpose of operation of a domain that has recognizably distinct existence (e.g., person, animal, service, passport, network device, software application or a website)".

Various attributes are sensed by sensing devices to identify entities in IoT. Furthermore, identified entities help supporting convenient intelligent services. Requirements for services' diversity and security catalyze the exploding growth of sensed entities and sensing devices. Under this tendency, the identification processes can be multiple. Apart from the pluralism of utility services, the diversification and large scale of Identification Exploding also result in a series of challenges [3].

There is a growing interest in building unified modeling to address the challenges of Identification Exploding. Modeling is responsible for describing things with the data from ubiquitous sensors (e.g., RFID, radar, and video sensor), and it can be used in identification [4]. Since Ning et al. [5] first introduced the concept of nID extending the ID-based identifiers, significant progress has been made to build unified solutions [6] [7]. Identification technologies (e.g., RFID, Single sign-on, Biometric, and Device Fingerprint) have been improved to identify ubiquitous heterogeneous entities accurately. JSON, XML, HTML, and XHTML are proposed to effectively describe identities' attributes for machine and human interactions. Besides, cloud-based computing(Software-as-a-Service) provides convenient services (e.g., coarse-grained information exchange) with compatibility beyond encoding methods. However, existed partial-solved issues have become more critical due to the lack of unified modeling for numerous entities covering various attributes across every domain. Although researchers have surveyed identity modeling and identity addressing methods [8], related works of the unified modeling still need comprehensive induction and analysis for further guidelines.

This paper provides a comprehensive review of the practice, challenges, and potential directions on unified modeling, aiming to help guide and shape future research. Section II introduces existing challenges of unified modeling. Section III analyses typical modeling methods widely used in IoT. Section IV evaluates modeling-based industry solutions under the resource-constrained environment, and the conclusions are drawn in Section V.

II. Background

As 5G technologies bringing increasing IoT-enabled business services, more entities swarm into the ubiquitous connections with various identity structures. It is imperative to build unified modeling for the exploding entities, each with heterogeneous identity structure carrying various attributes. Over time and space, identity data keep exchange across

TABLE I: Challenges of Unified Modeling

	Requirement	Challenge
Sensed Entity	Adopting to massive volumes and exploding proliferation	*Security and privacy*: Exploding identification requests with weak security protection left proliferative risks for possible cyber attacks and data theft.
		Mobility: The ubiquitous connection between mobile entities requires identification to be both flexible and robust during the migration of spatial locations and platform applications.
	Addressing heterogeneity and redundancy	*Heterogeneity and redundancy*: Heterogeneous entities owning various attributes are encrypted into different data structures, which impedes the integration and analytic with noises from the acquisition and transmission. The similarities and differences of entities' attributes in various domains lead to the waste of space for redundant storage and data inconsistency bringing extra management costs.
Sensing Device	Utilizing constrained resources in IoT environment	*Relative constrained resources of perception, computation. communication*: Traditional constrained sensing devices lack adequate computing resources to provide advanced sensing abilities for the complicated identification process. Modern sensing devices are hampered by limited network connectivity and high manufacturing costs that prevent them from performing as well as they should.
	Providing convenient identification, addressing, and exchange	*Interoperability*: Concerning four essential interoperability components (syntactic transformation, domain transformation, semantic transformation, and contextualization), existed IoT devices are still struggling with the requisite standards for unification.
		Scalability and compatibility: Without major modifications to sensing devices, new sensed entities can't be identified and addressed. And the widely used strategy "Embrace-Extend-Extinguish" further limits compatibility for exchange.

sensed entities and sensing devices. In this case, ubiquitous heterogeneous identities, insecure network channels, relative constrained sensing resources, standard mergers with monopoly tends, and data friction on content contextualization all pose a challenge to the unified modeling.

For sensed entities in cyberspace and physical space, where identity proliferates exponentially, various attributes have been extracted, encrypted, and compiled into specific data structures. However, identifiers are only subsets of attributes for the convenience of usage and management on a single platform. Clumsy fixed identification methods further impede the transmission and increase security risks and the possibility of privacy disclosure. To unify existed identification modeling for entities in different domains, heterogeneous and inconsistent attributes have become the primary concern. No solutions have been proved to achieve the proper balance between storage space and processing time.

For sensing devices, considering the constrained resource (i.e., perception, computation, and communication), existing schemes still take pre-defined values as the primary identification methods, which ensures stability and security but sacrifices flexibility. Although more feature-based identification modeling methods are investigated for smart devices, they are still in the experimental stage. In addition, the changeable environment further aggravates the difficulty of creating the unified modeling methods. Existing technologies cannot fundamentally remove the obstacle of a vicious competition strategy to the cross-device and cross-platform intercommunication of identification, addressing, exchange. With incompatible standards, devices are separately identified as individuals or alliances in non-uniform data format. The specific challenges of unified modeling are explained in Table I.

III. Identification Modeling for Ubiquitous Entities

This section presents key IoT identification modeling methods for sensed entities and sensing devices. There are more modeling methods presented in academic papers and conference discussions. Due to space limitation, six of them are summarized to represent the main approaches on how to model identities of sensed entities and sensing devices, what drawbacks existed methods have, and where the identification modeling evolves.

A. Sensed entities

1) Product-Related Identification Modeling
(PRIM) At the beginning, sensed entities in IoT were only physical products without lightweight computing memory chips inside and stable fast network support, such as goods in logistics or retail/wholesale [9]. Necessary information such as space-time data and manufacturing data are most commonly used to identify these products. They are encoded by human experience and cognition through heuristics. Tags are constructed with storage functions for identification to map the encoded entities' characteristics into their digital identity. The encoding methods of the given information are encoded by standardization organizations consisting of industry leaders like Wal-Mart, Hewlett-Packard, Cisco Procter & Gamble, and Lockheed-Martin, etc [10].

Because of the inevitable drawbacks (e.g., insufficient information storage ability and easily damaged) of the

traditional tags (e.g., EAN, GS1, UPC, Code128, matrix, and QR Code), RFID has been quickly developed into the mainstream in the context of IoT. During the competition of various manufacturers realizing precise requirements of multiple application scenarios, mature identification technologies (i.e., EPC, OID, and uCode) successfully weave themselves into the fabric of everyday life. The primary attributes encoded in the data carrier, such as space-time information and manufacturing information, representing products' birth, are widely used as the key components for identification. Regardless of read-only tags or erasable tags, entities' identity was ensured at one specific moment, e.g., manufacture completed, entities born, identities created. Considering privacy and security, additional artificial regulation and unified regulation are also need to model product-related entities' identities.

2) Inherent Characteristics based Identification Modeling (ICIM)

As entities with higher intelligence increase in the IoT, the inherent characteristics are abstracted to identify the entities. Such characteristics include biological characteristics, physical characteristics, chemical characteristics and specific abilities (completing the cryptography computation task [11], proving various functions [12], etc.).

In addition to physiological and behavioral characteristics (e.g., face, fingerprint, hand, iris, DNA, keystroke, signature, and voice), electrocardiograph, photoplethysmography, and electromyography are also promising approaches for continuous identification [13]. Also, zero-knowledge proof [14], hash function calculation [15], and even quantum computing [16] beyond the existing computing proneness are developing into solutions on mathematical tasks to prove computational abilities and unique hardware resources for identification. However, entities' characteristics are not stable eternally. There is a possibility of change and even the inherent characteristics can dissipate. Unless combining other identification mechanisms and policies, the flexibility of ICIM is more inadequate than the static characteristics.

3) Multi-Attributes based Identification Modeling (MAIM)

In this model, multi attributes behind the entities' digital shadow are unified together into the unique root certification recognized by Identity providers for cross-platform identification [17]. The root certification is the abstraction for all identifiers consist of multiple attributes. Identifiers with interchangeable encoding methods can reduce management stress and carry the load of identification on various entities with better coordination on services [18]. By combing various attributes into the unified data structure, the identification process could be more secure against attacks according to the USA Federal Regulators, approved by the Federal Financial Institutions Examination Council in their report [19].

Two mainstream solutions to implement MAIM for sensed entities are proposed separately from academia and industry. Researchers are trying to create an ideal identifier mapped with all attributes, including ID and nID. Chen et al. [20] built a mixed identifier consisting of a set of general information, i.e., identifiers, access information, credentials, attributes for sensed physical entities. Ning et al. [4] designed tree-code modeling and addressing methods for all ontology entities using RDF triples. Sahraoui et al. [21] proposed a mapping model that incorporates the cyber entity evolution and temporal parts consistency using a smart home as a use case scenario. In industry, the primary purpose is to meet existing identification mechanisms and mainstream frameworks' requirements. Hence, the universal certifications (OpenID, SAML, etc.) recognized and operated by industry leaders' alliances are the existing solutions. Implemented by the Public Key Infrastructure (PKI), certificates are issued to all entities under the same domain by Certificate Authority (CA). However, when implemented into ubiquitous heterogeneous IoT entities, existing MAIM methods are still limited in specific fields [22] because of the unavailable trade-off between efficiency and cost.

B. Sensing devices

1) Pre-defined Value based Identification Modeling (PVIM)

Although the diversity and scale of sensing devices keep increasing, PVIM has been accomplished for a long time. As the organ sensing entities in the Internet of Things, sensing devices are deployed all over the network. Therefore, in the actual communication process, pre-defined value is needed to ensure the reliability of sensed entities' attributes for sensing devices. At first, IoT devices were only recognized as common fixed nodes in a supposedly secure enclosed network. Identification was controlled via IP [23] based on the device whitelist. With the advent of brand new mobile smart devices, value including unique serial numbers, subscriber identity numbers are embedded in the SIM to provide higher mobility. Nowadays, even the essential Media Access Control (MAC-48/EUI-48) [24] has expended itself into the RFID tags to broader devices. Industrial devices are pre-embedded with Root of Trust during manufacture.

Explicit identifiers (IP, MAC, NFC, PKI, SIM, and RFID) are defined to carry pre-defined value for communication based on the vendors, birth certificate, manufacturer info, error-correcting codes. Although devices were broken, the identity could remain alive [25]. Due to the low cost and high flexibility, PVIM played a significant role in identifying resource-constrained sensing devices in the early stage. However, the open interconnected internet with ubiquity cyber attacks (Sybil Attack, Man-in-the-Middle Attack, Denial of Service, Device Spoofing, etc.) increase the possible security risks. For example, an ioctl systems call can help to forge or modify MAC address of the network interface card as devices identified by MAC addresses. Also, other IoT nodes using spoofed IP address can launch crucial attacks to acces sible devices in communicating. Generally speaking, these pre-defined values based identifiers can be altered or manipulated by using expert knowledge of network or software, causing security threat in identification between

machine-to-machine.

2) Intrinsic Features based Identification Modeling (IFIM)

In a particular environment requiring correct functioning and novel performance (i.e., Smart City, Smart Healthcare, and Industry 4.0), sensing devices are not worthy of pre-defined value representing the external trust unilaterally [26]. They have to prove their ability with no misbehavior detected during the identification considering risks of system faults, cyber attacks, hardware failure, etc. IFIM uses hardware functionality and behavior signatures to map intrinsic features to an anonymous-possible identity.

There are four mainstream device identification methods in IFIM, device fingerprint [26], behavior signature [27], environment check [28], and PUFs [29]. All of them are using multiple challenges to extract diverse hardware features from multiple domains and comparing them with different methods, e.g. rule-based, statistical, knowledge-based, time series, and machine learning. Although many proposals available, feasible schemes based on IFIM are still polarized. Traditional IoT sensing devices have not been compatible because of insufficient resources for proving their unique hardware features and new devices' types are too diverse to agree on general solutions without the unified standards.

3) Multi Proof-based Identification Modeling (MPIM)

In MPIM, devices map multi proof group representing identity credibility of the sensing devices, taking external trust from the pre-defined value, and proving itself with the intrinsic features. As one of the promising identification options for IoT sensing devices, MPIM has powerful security mechanisms and fast transmission performance.

Due to limitations in technologies and policies, academia and industry still investigate a flexible universal solution for MPIM. Existent research in implementing MPIM is more of a variant or optimized version of methods in IFIM. For example, IoT-ID [30] implements pre-defined value for resource-restrained IoT devices based on internal PUFs from Analog to Digital Converter and clock oscillators. Most importantly, it could be compatible with traditional IoT sensing devices without extra circuit elements providing storage for identification. However, the number of devices increases the likelihood of multiple devices having the same ID increases with system components' bounded process variations. Hence, there are still a lot of challenges waiting to be solved for researchers to improve MPIM towards a unified solution for sensing devices.

IV. Modeling-based solutions under resource-constrained IoT environment

This section presents the resource-constrained IoT environment. By reviewing model-based industry solutions, this paper explored the solutions to existing challenges and abstracted the unified modeling's key points.

A. Resource-constrained IoT environment

Conventional modeling methods based on external trust borrow necessary resources from central controllers. Fresh new smart entities generate proofs from tapping into internal potential for identification. To some extent, existing identification schemes do successfully identify heterogeneous entities. But in the context of IoT, the identification modeling still suffers from three significant limitations: 1) constrained sensing resources, 2) limited computing ability, 3) limited communication resources.

During the modeling process, sensing devices first need to extract attributes of entities to describe identity in a particular domain as distinct from other entities'. Manufacturers are likely to equip IoT devices with low-power embedded computational modules to minimize the cost. Hence, low storage capacity limits the variety of intelligent sensing functions. Due to the lack of sufficient perceptive resources, devices fail to detect enough attributes of entities for accurate, intelligent identification in particular application scenarios (e.g., industrial control and monitoring, home automation, security and military sensing, asset tracking and supply chain management) [31]. Approaches such as compressive sensing (CS), intelligent sensing, and selective sensing have improved the sensing ability with low-cost resources. As a new sensing modality, CS compresses the acquired signal at the sensing time to less than the Nyquist sampling rate. With big data and multiuser-detection, CS shows good performance in reducing energy consumption. By improving devices' intelligence, smart sensing reduces the consumption of data transmission [32]. By adding signal processing ability of onboard sensor, devices could make effective local decision in sensing data incorporating multiple sensing modules producing multi-intellectual output. Selective sensing [33] borrows the biological attention mechanism to give IoT devices novel selective sensing ability in a noisy environment. It can be deployed in the application scenario of large-scale sensor explosion data transmission, reducing the consumption of resources caused by irrelevant perceived noises in the original data processing.

After sensing various features, devices need to achieve the internal identity information. However, analyzing perceptual attribute data would impose a time and computational burden on small, battery-powered IoT devices. Hence, machines tend to seek additional help from the cloud to make up for their lack of computing resources. In 2014, Karim Arabi put forward the idea of edge computing [34]. Researchers suggested that network nodes owning redundant computing power could help IoT devices accelerate identification by efficiently providing edge storage and calculation to process heterogeneous data. Similarly, fog computing uses nodes between cloud and edge nodes to reduce data processing delays [35]. In addition to saving power consumption, these autonomous nodes support wide-spread geographical distribution networks and content distribution. In the case of no internet connection, dew computing provides pooled computing capacity by combining functional components bearing micro-services. And ad-hoc based

TABLE II: Evaluations for modeling-based Industry Solutions

	Name	Model	Scenarios	Description	Characteristics				
					S	H	A	C	I
Sensed Entity	GTIN	PRIM	Transportation and Logistics Management/	The global trade item number (GTIN) consists of company prefix, a calculated check digit, and item reference. By incorporating ISMN, ISBN, ISSN, and UPCs, GTIN builds a universal digital space beyond organizational boundaries.	×	×			
	Evrythng	ICIM	Retail/ Wholesale	In Evrythng, a unique Active Digital Identity™ (using RFID and QR code) is assigned to the physical product for identification, referring to various inherent attributes with metadata.			×	×	
	SAML	MAIM	Web Services	Consisting of attributes for authentication and authorization, SAML help provide assertion for multiple service providers to prove the user's identity. Its universality has been steadily increasing with more optional criteria.				×	
Sensing Device	oneM2M	PVIM	Smart Home	oneM2M is an international standard organization in the IoT field of M2M communication. It uses external trust to identify devices ID with a prefix based on OID consisting of device type, serial number, and manufacturer.	×				×
	Intrinsic Id	IFIM	E-Commerce	Intrinsic ID provides a digital authentication method using SRAM PUF to authenticate devices' internal chips. It is widely used to validate payment systems, secure connectivity, authenticate sensors in IoT systems.		×	×		
	Watson IoT	MPIM	Industry 4.0	This platform builds Client ID combing external trust and the internal proof to identify users' devices, including token, device type, device ID, operation ID, URL.			×		

networking technologies are used for computation and connection to eliminate the network topology restriction. These sub-classes of distributed computing alleviate IoT devices' limited computing power, reduce time, and improve efficiency by calling adjacent devices' resources.

Finally, identity data needs to be sent back to the server for backup. Most of embedded IoT devices owning 8-bit or 16-bit microcontrollers have insufficient RAM and storage capacity. Hence, solutions such as compression, aggregation, and filtering have been used to reduce and minimize data transmission burden. IETF has developed the 6LoWPAN standard to improve limited communication resources, allowing IPv6 packet to switch over an IEEE 802.15.4 link with shorter forwarding delay. Hence, the purpose-built protocols (CoAP [36]) could be implemented on top of the IPv6 infrastructure. Existed network protocols for these devices are also recompiled for constrained devices to fit the traditional framework, allowing all current tools to remain functional and applicable.

B. Modeling-based Industry Solutions

Even under resources-constrained environments, there are still a series of modeling-based industrial solutions proposed to address challenges brought about by the Identification Exploding. By referring to the official documents and relevant evaluation at www.g2.com, six from 30 industry solutions are selected according to modeling, application, and characteristics (Security, Heterogeneity, Agility, Consistency, and Interoperability). The mobility, scalability, and compatibility have been united into the agility to eliminate the overlap and increase an entity's application scope. On this basis, this paper further examines each solution based on the research challenges presented above. The evaluation and comparison are shown in Table II, where characteristics are abbreviated by their English initials.

The existed modeling-based industry solutions' emulations reveal two key conclusions: 1) Solutions based on the MAIM and MPIM show superiority over others by combining external trust and internal capability. 2) Existed identification modeling are limited to specific local domains of entities, devices, or providers because of the restraint policies, technologies, and market. At the same, there is no perfect solution to meet all the evaluation indexes.

From analyzing these methods, this paper can draw a number of findings. First, identification modeling is a process of attributes mapping involving the issue of trust in essence. Two forms are adopted: one is the external recognition and the other is to prove itself through internal ability. In the past, entities in IoT are only lifeless commodities carrying external trust. But the resurgence of artificial intelligence after a 30-year incremental development has given a new definition to entities with intellectual ability. At the same time, exploding identities also increase the demand on verify external trust. One unique entity may have multiple identities, and different entities may appear in the same sensor network. Accordingly, by mining intrinsic attributes from entities, new identification methods are proposed to address emerging new challenges. MAIM, MPIM both combine the external trust with internal proof in some ways for identification. As a result, they both show better performance in solving challenges.

However, during the unification process, these two attributes sets are not equal. More often than not, the internal proof is only additional verification stored in the external trust certifications. This unified pattern demonstrates that identity providers have absolute control over the trust and data, impeding data exchange and cross-domain cooperation for Big Data. The Information isolated islands are rising with more data friction. Existing local unified modeling methods are built-in independent exchanges space for the resource integration from industry leaders or the national sectors. Although they capture two vital elements of external trust and internal ability, a reasonable, efficient, achievable, and beneficial solution that identifying each entity is still lost. It still has great research value and development potential to construct a global unified modeling system for various IoT scenarios.

V. Conclusion

IoT is experiencing an "Identification Exploding" caused by "Entity Exploding" and "Connection Exploding" of ubiquitous entities. With the improvement of sensing technology, heterogeneous attributes are utilized for identification to provide precise services. Nevertheless, diversity also increases the difficulty of unification. The growing demand for entities' identity services brought too much burden to the resource-constrained IoT devices for carrying complex, reliable identifiers. This paper explores the existing challenges in the path towards the unified modeling across attributes, entities, and domains. It then introduces basic identification modeling to get the basic sets, external trust, and internal proof. Finally, model-based industry solutions are evaluated to guide unified modeling under Identification Exploding. With the unified modeling process for various entities, IoT could move the development process from sensing intelligence to cognitive intelligence. Different devices from different manufacturers will be able to achieve seamless communication and cooperation. Most importantly, IoT services could evolve intelligently through the entity identification data's actual value with clear ownership under rules' binding.

References

[1] "State of the iot 2018," 2018, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

[2] "The mobile economy," 2020, https://www.gsma.com/mobileeconomy/.

[3] H. Ning, F. Shi, S. Cui, and M. Daneshmand, "From iot to future cyber-enabled internet of x (iox) and its fundamental issues," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[4] H. Ning, Y. Fu, S. Hu, and H. Liu, "Tree-code modeling and addressing for non-id physical objects in the internet of things," *Telecommunication Systems*, vol. 58, no. 3, pp. 195–204, 2015.

[5] H. Ning, S. Hu, W. He, Q. Xu, H. Liu, and W. Chen, "nid-based internet of things and its application in airport aviation risk management," *Chinese Journal of Electronics*, vol. 21, no. 2, pp. 209–214, 2012.

[6] H. Ning, X. Liu, X. Ye, J. H. W. Zhang, and M. Daneshmand, "Edge computing based id and nid combined identification and resolution scheme in iot," *IEEE Internet of Things Journal*, 2019.

[7] P. Hu, H. Ning, T. Qiu, Y. Xu, X. Luo, and A. K. Sangaiah, "A unified face identification and resolution scheme using cloud computing in internet of things," *Future Generation Computer Systems*, vol. 81, pp. 582–592, 2018.

[8] H. Ning, Z. Zhen, F. Shi, and M. Daneshmand, "A survey of identity modeling and identity addressing in internet of things," *IEEE Internet of Things Journal*, 2020.

[9] J. P. Ruppert, R. C. Fish, T. A. Yap, and R. M. Ames, "Portable rf id tag and barcode reader," Jun. 17 1997, uS Patent 5,640,002.

[10] M. Baudin and A. Rao, "Rfid applications in manufacturing," 2000.

[11] M. O' Neill *et al.*, "Insecurity by design: Today' s iot device security problem," *Engineering*, vol. 2, no. 1, pp. 48–49, 2016.

[12] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, vol. 43, no. 2, pp. 90–98, 2000.

[13] A. Barros, D. Rosário, P. Resque, and E. Cerqueira, "Heart of iot: Ecg as biometric sign for authentication and identification," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2019, pp. 307–312.

[14] G. Park, B. Kim, and M.-s. Jun, "A design of secure authentication method using zero knowledge proof in smart-home environment," in *Advances in Computer Science and Ubiquitous Computing*. Springer, 2016, pp. 215–220.

[15] A.-I. Radu and F. D. Garcia, "Leia: A lightweight authentication protocol for can," in *European Symposium on Research in Computer Security*. Springer, 2016, pp. 283–300.

[16] T. M. Fernández-Caramés, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2020.

[17] A. Jøsang and S. Pope, "User centric identity management," in *AusCERT Asia Pacific information technology security conference*. Citeseer, 2005, p. 77.

[18] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 553–567.

[19] "Ffiec press release." http://www.ffiec.gov/press/pr101205.htm.

[20] J. Chen, Y. Liu, and Y. Chai, "An identity management framework for internet of things," in *2015 IEEE 12th International Conference on e-Business Engineering*. IEEE, 2015, pp. 360–364.

[21] S. Dhelim, N. Huansheng, S. Cui, M. Jianhua, and I. K. Wang, "Cyber-entity and its consistency in the cyber-physical-social-thinking hyperspace," *Computers Electrical Engineering*, vol. 81, p. 106506, 2020.

[22] P. Dash, C. Rabensteiner, F. Hörandner, and S. Roth, "Towards privacy-preserving and user-centric identity management as a service," in *Open Identity Summit 2017*, L. Fritsch, H. Roßnagel, and D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2017, pp. 105–116.

[23] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of resource constrained devices in the internet of things," *Communications Magazine IEEE*, vol. 50, no. 12, pp. 144–149, 2012.

[24] IEEE, "Ieee registration authority-faqs," https://standards.ieee.org/faqs/regauth.html.

[25] R. R. Chowdhury, S. Aneja, N. Aneja, and E. Abas, "Network traffic analysis based iot device identification," *arXiv preprint arXiv:2009.04682*, 2020.

[26] P. M. S. Sánchez, J. M. J. Valero, A. H. Celdrán, G. Bovet, M. G. Pérez, and G. M. Pérez, "A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets," *arXiv preprint arXiv:2008.03343*, 2020.

[27] B. Bezawada, M. Bachani, J. Peterson, H. Shirazi, I. Ray, and I. Ray, "Iotsense: Behavioral fingerprinting of iot devices," *arXiv preprint arXiv:1804.03852*, 2018.

[28] Y. Meidan, M. Bohadana, A. Shabtai, D. J. Guarnizo, M. Ochoa, O. N. Tippenhauer, and Y. Elovici, "Profiliot: a machine learning approach for iot device identification based on network traffic analysis," *SAC*, pp. 506–509, 2017.

[29] J. Delvaux, R. Peeters, D. Gu, and I. Verbauwhede, "A survey on lightweight entity authentication with strong pufs," *ACM Computing Surveys (CSUR)*, vol. 48, no. 2, pp. 1–42, 2015.

[30] G. Vaidya, A. Nambi, T. Prabhakar, S. Sudhakara *et al.*, "Iot-id: A novel device-specific identifier based on unique hardware fingerprints," in *2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2020, pp. 189–202.

[31] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of resource constrained devices in the internet of things," *IEEE Communications Magazine*, vol. 50, no. 12, pp. 144–149, 2012.

[32] F. Al-Turjman and S. Alturjman, "Confidential smart-sensing framework in the iot era," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 5187–5198, 2018.

[33] H. Ning, X. Ye, A. B. Sada, L. Mao, and M. Daneshmand, "An attention mechanism inspired selective sensing framework for physical-cyber mapping in internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9531–9544, 2019.

[34] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, and E. Riviere, "Edge-centric computing: Vision and challenges," 2015.

[35] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. S. Goren, and C. Mahmoudi, "Fog computing conceptual model," Tech. Rep., 2018.

[36] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," 2014.