A Survey of Identity Modeling and Identity Addressing in Internet of Things

Huansheng Ning, *Senior Member, IEEE*, Zhong Zhen, Feifei Shi, and Mahmoud Daneshmand, *Life Senior Member, IEEE*

***Abstract*—With the development of the Internet of Things (IoT), the physical space we are living in is experiencing unprecedented digitalization and virtualization. It is an overwhelming trend to achieve the convergence between the physical space and cyberspace, where the fundamental problem is to realize the accurate mapping between the two spaces. Therefore, identity modeling and identity addressing, which serve as the main bridge between the physical space and cyberspace, are regarded as important research areas. This article summarizes the related works regarding identity modeling and identity addressing in IoT, and makes a general comparison and analysis based on their respective features. Following that a flexible and low coupling framework, with strong independence between different modules is proposed, where both identity modeling and identity addressing are integrated. Meanwhile, we discuss and analyze the future development and challenges of identity modeling and addressing. It is proved that identity modeling and identity addressing are extremely significant topics in the era of IoT.**

***Index Terms*—Identity addressing, identity modeling, Internet of Things (IoT).**

I. Introduction

THE Internet of Things (IoT) is a universal and adaptive network establishing ubiquitous connections between different sensors, devices, and other objects. It is one of the most important areas and plays a significant role in the development of society and technology. The IoT holds an important position in achieving interconnections between the physical space and cyberspace and contributes a lot in realizing the whole convergence. The fundamental problem during the convergence is to realize the accurate mapping between the two spaces and effectively handle and find massive cyber entities, thus achieving the bidirectional flow of data and information. This requires consistency in identity modeling, fast and accurate identification, as well as full addressing and recognization. Therefore, identity modeling and identity addressing become one of the most basic and key components of the IoT.

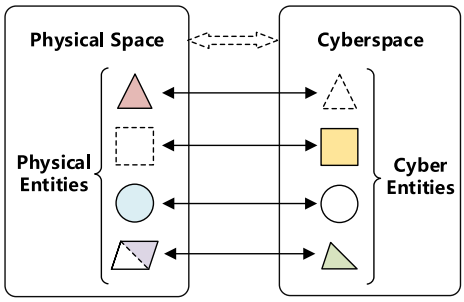

Fig. 1. Entities and their relations in the cyberspace and physical space [1].

Entities in the physical space are mapped to cyber entities in the cyberspace through identity modeling, and cyber entities act on the physical space for interaction and control. Therefore, the identity modeling mentioned in this article is to model the entity of the physical space, and identity addressing is to address the entities in the cyberspace. Relevant scholars, Ma *et al.* [1] and Dhelim *et al.* [2], have put forward the relationship between physical entities and cyber entities. The identity modeling and addressing introduced in this article are based on the entities in Fig. 1. There are several relationships between the physical entities and the cyber entities. There are entities in the physicalspace and cyberspace that are not mapped in the corresponding space, or basic mapping and complementary mapping.

In the traditional design of the IoT, the identity modeling is usually marked by designing the encoding method and physical carriers, such as radio frequency identification (RFID) [3] or barcode, and identity addressing is based on the domain name system (DNS) [4] service. With the continuous increase of demanding requirements, as well as the explosive complex markups and unmarkable entities, establishing identities and achieving accurate identity addressing for heterogeneous resources are becoming more prominent. These problems have brought great challenges to the development of the IoT.

IoT implements overall interconnections with a variety of technologies ranging from low-level sensor devices to high-level servers, from human–machine interactions to machine–machine interactions. The identity modeling needs to consider

Manuscript received September 28, 2019; revised January 21, 2020; accepted January 28, 2020. Date of publication February 5, 2020; date of current version June 12, 2020. This work was supported in part by the National Natural Science Foundation of China under Grant 61872038 and Grant 61811530335, and in part by the Civil Aviation Joint Funds of the National Natural Science Foundation of China under Grant U1633121. *(Corresponding author: Huansheng Ning.)*

Huansheng Ning is with the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China, and also with the Beijing Engineering Research Center for Cyberspace Data Analysis and Applications, Beijing 100083, China (e-mail: ninghuansheng@ustb.edu.cn).

Zhong Zhen and Feifei Shi are with the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China.

Mahmoud Daneshmand is with the Department of Business Intelligence and Analytics and the Department of Computer Science, Stevens Institute of Technology, Hoboken, NJ 07030 USA.

Digital Object Identifier 10.1109/JIOT.2020.2971773

the entities that can be queried more efficiently in cyberspace, but also support more efficient queries and intelligent services and reduce data friction [5]. A core element for identity modeling is the data carrier. For traditional entities, physical entities are tagged by physical carriers, such as RFID or barcodes. As technology improves, the identity modeling methods gradually deviate from the physical carriers, and begin to focus on data carrier-based modeling methods to identify the entities, which include various attributes, including color, shape, features, etc. At the same time, the identity modeling method gradually develops from the traditional label to the triple tuple based on the semantic Web. The identity modeling based on this method can better express the relationship between cyber entities and has good support for the development of intelligent services. Identity addressing means the process of querying cyber entities in cyberspace and finding corresponding entities in the physical space. The identity addressing in IoT solution inherits a lot from the Internet addressing solution. Therefore, by investigating and surveying the traditional addressing methods in the Internet, the core identity addressing structure is extracted and analyzed from Internet addressing. It also provides a solution for heterogeneous resources addressing and intelligent addressing. This article not only summarizes the technology of identity modeling and addressing but also puts forward some noteworthy matters in the specific identity modeling and addressing. At the same time, aiming at the status of identity modeling and identity addressing in IoT, a flexible and low-coupling identity modeling and addressing framework of IoT are proposed. Finally, several aspects in the field of identity modeling and addressing are proposed, and the future prospects and challenges are discussed and analyzed, as well as the future network architecture and security privacy.

The remainder of this article is organized as follows. Section II introduces the identity modeling schemes in IoT. Section III illustrates the identity addressing schemes in IoT. Section IV presents a unified framework with integrating identity modeling and identity addressing modules. Section V puts forward some open issues, prospects, and challenges for the current development of identity modeling and addressing. Section VI summarizes this article. Fig. 2 outlines the structure of this article.

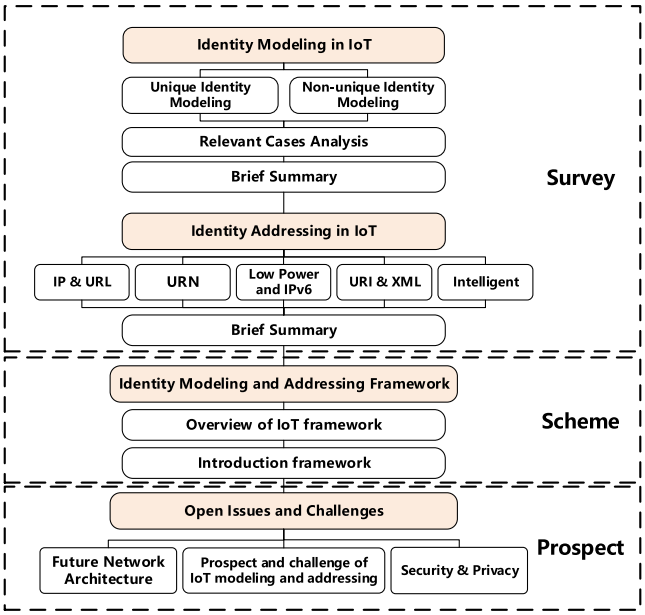

Fig. 2. Diagram of the structure of this article.

II. Identity Modeling in IoT

When we deploy sensors and other devices in the physical world and connect them to the cyberspace, the key problem is identifying those entities. Here, we will use the word "entity" to express the natural creatures, concrete and abstract things, events, cyber resources, etc., in cyberspace and physical space, and envisage that all physical entities can be mapped in cyberspace as much as possible. In order to provide an efficient and fast identification and retrieval method, we need to design a storage rule, a crucial factor to be considered in the identity modeling of IoT. Similarly, identity modeling provides a unique serial number for cyber entities and reduces data friction between people and machines in a way. This section introduces identity modeling in two parts, unique identity modeling and nonunique identity modeling, and then summarizes various modeling methods through reference research. In the end, various types of modeling methods are summarized.

A. Unique Identity Modeling

In the beginning, identity modeling in IoT establishes a mapping from the physical world to the cyber world by unique modeling. Unique identity modeling refers to the construction of unique identity through certain coding rules, or some natural attributes.

In cyber and physical space, constructing tags into objects is a necessary condition for objects in physical space to communicate and interact with cyberspace. Building a tag requires designing a data carrier and encoding information. Common data carriers are 1-D barcodes, 2-D codes, uniform resource identifiers (URI) [6], device memories, and RFID tags. Common 1-D codes are EAN/UPC, ITF-14, UUC/EAN-128, and GS1 DataBar. Common quick response (QR) codes are QR Code, Data Matrix, PDF417, Postal Codes, and more. For electronic tag RFID, there is currently no uniform RFID encoding rule in the world, mainly including the following types of standards: EPC [7], uCode [8], and OID.

However, in the actual system, a lot of entities do not have any ID number attached, or it is difficult to obtain the existing ID number, because there is no appropriate reader. In this case, ID-based IoT solutions become inapplicable. Faced with such challenges and complex demands brought about by the development of technology, the data carrier has gradually deviated from the traditional labeling method. People began to take the attributes and features of the object itself as data carriers, such as physical signal, fingerprints, pupils, behavioral characteristics, etc. Collecting these features can also be obtained through various sensors or other means.

Therefore, the identity modeling method has achieved a novel breakthrough. Ning *et al.* [9] proposed nID to represent

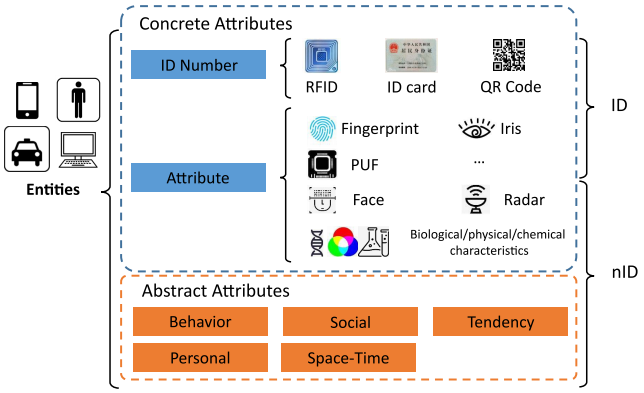

Fig. 3. nID schematic.

such physical objects that cannot be identified by ID coding. Then they [10] proposed a tree-code model, a physical object modeling scheme that supports emerging nID data elements and is compatible with ID data element modeling, as shown in Fig. 3. This solution offers a good idea in the direction of identity modeling in IoT. However, it faces challenges in terms of space–time consistency and addressing time. Kwok *et al.* [11] applied Physi-ID to the identification of physical objects based on the identification of physiological features. This concept improves the accuracy in the identification of physical objects by verifying their unique physical and chemical properties.

The physical unclonable function (PUF) is a promising technology whose response to input stimuli is easy to measure but difficult to clone. Nonclonality is the hardness that is accepted by replicating a large number of uncontrollable manufacturing characteristics and enables PUF to help solve issues, such as authentication, software protection/licensing, and certification enforcement [12]. Dong *et al.* [13] proposed a device fingerprint scheme based on the CPU performance graph. At the same time, the PUF technology can be used to model the identity of hardware devices, and it has a good application in the recommendation system of the e-commerce field.

B. Nonunique Identity Modeling

The traditional identity modeling method is a simple and efficient identity modeling method, easy to manage and operate, and it solves the data friction between people and machines. However, due to its structural limitations, that method cannot express the data hierarchy and the relationship between data, nor is it competent for complex query requests. The nonunique identity modeling method can be used to identify entities by describing their attributes. The complex attributes in daily life are constructed and correlated to form a kind of content that can be understood and processed by human and machine, and then analyzed, excavated, and reasoned.

First, we will introduce the markup language technology, such as XML and JSON. This type of technology provides a unified way to describe and exchange structured data that is independent of the application and is an important language for network data representation and exchange. There is a sensor model language (SensorML) [14] model provides a standard model and XML encoding. SensorML can be used to describe sensors, including dynamic and stationary platforms, as well as *in-situ* and remote sensors. The main objective is to enable interoperability so that machines can better understand sensors and processes, automatically use sensors in complex workflows, and easily share intelligent sensor Web nodes between them. There is also UML, an open method for explaining, visualizing, building, and object-oriented open methods. UML is proven to be effective in the modeling of large and complex systems, especially at the software architecture level, and represents a set of best engineering practices. For example, Prehofer pioneered the use of sensors and actuators in the UML model to model complex IoT systems and generate RESTful interfaces. As is shown in software development in embedded domains, advanced models can significantly increase productivity [15].

The semantic Web [16] combines the data and demand characteristics of the IoT and provides a more general modeling method than the above. The foundation of semantic Web knowledge representation and reasoning is ontology, which is used to describe how classes, instances, and their attributes are defined, described, and related. By elevating data to knowledge through a common ontology language, data can be better shared and reused. Next, we will introduce the ontology description language and related content recommended by World Wide Web Consortium (W3C). Szilagyi and Wira [17] have a good explanation of the ontology concept and the Semantic Web.

RDF [18] provides a unified standard for describing resources on the Web, such as classes, properties, instances, and so on. RDF is formally represented as a subject–predicate–object (SPO) triple. After understanding the representation and type of RDF, the next step is to serialize RDF. That is to store and transmit RDF data. Commonly used methods are: RDF/XML, N-Triples, Turtle, RDFa, JSON-LD, etc., among which Turtle is used more widely. Hasemann *et al.* [19] built a Wiselib RDF Provider platform that introduced Streaming HDT, a lightweight serialization format for RDF documents that allows compressed documents to be transferred with minimal coding effort. Gutierrez *et al.* [20] introduced time into RDF reasoning.

RDF is used to describe the relationship between resources, but there is no definition of hierarchical relationships between classes. RDFS [21] has improved in this regard. RDFS adds vocabulary to RDF based on RDF to extend the capabilities of RDF so that users can standardize the classes and attributes in a particular domain and then standardize the description of RDF.

Due to the weak expression of RDFS, the W3C released the Web ontology language (OWL) in 2004 [21]. OWL adds additional vocabulary to describe resources and has better semantic expression capabilities. The core of OWL's design is to find a reasonable balance between language expression and intelligent services (such as reasoning). OWL has three increasingly expressive sublanguages: 1) OWL Lite; 2) OWL DL; and 3) OWL Full. Later in 2012, W3C published the technical specifications of OWL 2 [22]. The core of OWL 2 is the description logic SROIQ, which is more expressive, but it also

increases some computational complexity. OWL 2 adds new functionality with respect to OWL. Such as syntactic sugar, and defined new profiles and syntax. Some restrictions applicable to OWL DL have been relaxed [23]. The Semantic Web stack shows the relationship between the languages described above.

The above is the ontology description language, while the following is the more common ontology. W3C has proposed two ontology languages, semantic sensor network (SSN) and semantic actuator network (SAN), for sensors and actuators. The SSN defines an ontology for describing the sensor and its observed variables, the involved procedures, the characteristics of the study, the samples used, the observed properties, and the executing mechanism [24]. SAN introduces actions, execution devices, execution characteristics, execution scope, and so on, and provides a wide range of concepts and properties for actuators [25]. IoT-O ontology, a core domain IoT ontology, extends with vertical, application-specific knowledge to model horizontal knowledge about IoT systems and applications. Its component modules include SSN and SAN and others [17].

Through the above identity modeling methods, we can better construct the semantic Web, so that the data conforming to the corresponding specifications is easily understood by the computer, thereby enabling more convenient sharing and data reuse between different applications or systems. The architecture constructed based on the rules of the semantic Web can form a knowledge/relational graph, which can effectively query and solve the problem of information overload and knowledge reasoning, and discover the implicit relationship. Ganz *et al.* [26] proposed a method of knowledge acquisition that automatically extracts rules and creates and develops topic ontology by acquiring sensor data. A knowledge graph is a hotspot of technology combined with big data intelligence. It is believed that the combination of this field and research of identity modeling in IoT will inevitably lead to many valuable research contents.

With the increasing demand for information sharing among industries and fields, cross-domain information exchange has become an important issue, and the difficulty of this problem is the heterogeneity of data. Many scholars solve the problem of semantic and grammatical inconsistencies by constructing a knowledge graph. Because of the complexity of information relations, there are also some difficulties in the implementation of real scenes. The national information exchange model (NIEM) [27] implemented jointly by the United States Department of Homeland Security and the United States Department of Justice has solved the problem of information exchange between different data formats. NIEM builds the NIEM data model by extracting and summarizing information in various fields. The information exchange parties establish information exchange specification that meets the requirements by citing and mapping the NIEM data model. At last, the information provider generates the information exchange package according to the information exchange specification and transmits it to the information receiver. The receiver parses the data in the information exchange package according to the information exchange specification so as to realize the information exchange.

C. Relevant Cases Analysis

In the above, we introduced the current mainstream method of identity modeling in IoT, but the IoT field covers a wide range, and the identity modeling method used should correspond to the actual demand scenario. Some identity modeling cases for the IoT have been proposed.

Yang [28] proposed an RFID-based warehouse management system that improves storage efficiency and reduces cost and energy consumption. Ning *et al.* [30] provided a semantic sensor-based network ontology that follows the accepted criteria for sensor data semantics in smart homes, including modeling sensors, context and semantic activities, and aggregating ontology with spatiotemporal information and user profiles. Gaur *et al.* [33] proposed a smart city architecture based on the semantic Web technologies and Dempster–Shafer uncertainty theory by studying how to better manage and analyze the data generated by wireless sensors in the smart city.

Khaled and Helal [34] proposed an inter-relationship programming framework that uses the Atlas transaction architecture and the IoT-DDL project to build a distributed programming ecosystem for the social IoT. The essence of IoT-DDL is an XML-based modeling approach. Abkenar *et al.* [31] proposed a model and specification language GroupSense-L for group activities, and a generic IoT-enabled architecture for analyzing sensor data aggregated from a set of nearby embedded sensors to identify and understand the characteristics of the group's activities. Its modeling method is a self-defined modeling method, and its ideas and application purposes are similar to RDF. Afzaal and Zafar [32] combined the IoT with frontier defense and used UML to the border protection system. Li *et al.* [35] analyzed the social attributes of things, and the role of social relationships, and used the super-network architecture to present complex relationships between physical things. They used an ontology-based approach to simulate the relationship of things. Based on this, a new breast cancer risk assessment model and the contraction model, were proposed. Under an uncertain classification standard, Shrink [36] used a grouping algorithm to identify high-risk groups of breast cancer to prevent and control breast cancer. In the field of social relations, Ning *et al.* [37] proposed and evaluated a novel friend recommendation system based on the Big Five personality model and hybrid filtering.

Bonacin *et al.* [29] described the OntoAgroHidro ontology, extracting the characteristics of events from space and time, and describing them in multiple dimensions to represent the knowledge of the impact of agricultural activities on water resources and the impact of possible climate change. Mohammed *et al.* [38] proposed an alignment algorithm and an efficient way to store and retrieve knowledge related to human diseases.

Through the above review of the identity modeling that has been put forward in recent years, we can find that the fields involved include traditional logistics and transportation industry, social life, group relations, social services (agriculture, medical care, security), etc. The seemingly complex modeling field can be classified into five main methods: 1) space-time; 2) behavior; 3) activities; 4) society; and 5) relationships. Many

TABLE I
SUMMARY OF IDENTITY MODELING SOLUTIONS

Classification	Field	Modeling Method	Reference
Space-time	Warehousing System	ID	[28]
	Risk Management	nID	[9]
	Agriculture	OWL	[29]
	Smart Homes	SSN	[30]
Behavior & Activities	Group Activity Recognition	RDF	[31]
	Border Protection	UML	[32]
Society & Relationships	Smart City	OWL	[33]
	Social IoT	SWRL (XML)	[34]
	Social Attributes	SWRL (XML)	[35]
	Medical Social Network	nID	[36]
	Social Computing	nID	[37]

identity modeling methods are not based on a single way. Here, through the above papers technology and scheme, we extract the essential identity modeling method and organize them as shown in Table I.

D. Brief Summary

In the above content, we introduce some identity modeling methods and related cases, and then we will introduce some noteworthy matters in the identity modeling process. In the practice of identity modeling of IoT entities, the first thing to think about is the field and requirements. Define the content and purpose of the build, and analyze what data forms are needed. Next, the data are modeled according to the scheme formed in the previous process, and then the model is evaluated in actual use, and the problems are improved. However, the modeling process of a perfect model is not accomplished at one stroke and it needs continuous iterative design. Do not think too much about the design at the beginning, resulting in the initial version is too complex, increasing the design difficulty; at the same time, we need to improve the main core content as much as possible, taking into account the future expansion. In the following, we will elaborate some matters that need attention in identity modeling from the perspectives of identification and semantics.

In the practice of the identity modeling process, the most important and fundamental requirement is to identify an entity. Through analyzing the application scenarios and requirements, we can choose which physical carrier to use. For example, human–device interaction can use visualized and convenient methods, such as QR, fingerprint, and iris. RFID, PUF, etc., can be selected for the object-device interaction for the data easy to collect. For coding protocols and standards, they need to be selected according to business scope, local policies, and addressing methods. In the coding process, there are also some requirements and noteworthy points: the coding should reflect the classification and order, and have scalability, and at the same time to ensure the length is consistent. A check bit is also necessary, it can effectively prevent errors in identification and entry. In addition, the meaningful numbering should be avoided in the coding process. Although it is convenient for people to identify the entity corresponding to the number, such design will lead to conflicts with the above requirements. In essence, numbering is to facilitate computer management and identification. The variable attribute in the code should not be included in the number. At the same time, some confusing contents should be prevented in the design code, such as 0 and *O* and l and 1, and some special symbols.

The construction and design of semantic identity modeling is also an important aspect. One of the important points is how to build the ontology model. Gruber [39] and Zhang [40] put forward five criteria, which are given as follows.

1) *Clarity:* Ontology should give a clear and objective semantic definition to the defined terms in natural language.
2) *Coherence:* The inference from the term is consistent with the meaning of the term itself, and there will be no contradiction.
3) *Extensibility:* There is no need to modify existing content when adding general or special terms to ontology.
4) *Minimal Encoding Bias*: The perception should be specified at the knowledge level.
5) *Minimal Ontological Commitment:* Given as few constraints as possible to the modeling object.

Arpirez *et al.* [41] added three criteria: 1) concept name standardization; 2) concept level diversification; and 3) semantic distance minimization. For the process of creating the ontology model, Noy and McGuinness [42] analyzed the early famous ontology design projects, and combined with their experience in developing and using a variety of ontology editing environments, gave a specific process of creating Ontology.

1) Determine the domain and scope of the ontology. In this step, some basic questions need to be clarified, such as: what domain does the ontology cover, what information to describe, what kind of questions to answer, and who will use and maintain the ontology.
2) Consider reusing existing ontologies. Finding the ontology related to requirements is a very useful thing. If the existing ontology can be refined, extended, or modified, many unnecessary development works can be avoided. Even if it is not found to meet the current application requirements, it will usually get some inspiration and help from it.
3) Enumerate important terms in the ontology. These terms generally indicate the objects of interest in the modeling process, the attributes of objects, and the relationship between them. These important terms ensure that the ontology created will not deviate from the field of interest.
4) Define the classes and the class hierarchy.
5) Define the properties of class slots. The top-down development process, bottom-up development process, and combination development process are introduced. No matter which method is chosen, we should start from defining classes, select terms abstracted from concrete objects as classes in ontology, and then construct classification hierarchy.
6) Define the facets of the slots. Some limitations of attributes need to be further defined, including the

cardinality of attributes, the types of attribute values, and the domain and value domain of attributes.

7) Create instances. Finally, create an instance for the class. This requires identifying the class closest to the individual, adding the individual as an instance of the class, and assigning values to the properties of the instance.

III. Identity Addressing in IoT

Cyberspace is an information carrier of physical space. Physical entities are mapped to cyber entities through identity modeling. When the mappings have been built, the next question is how to find these cyber entities. This section classifies and summarizes identity addressing from its technical essence, introduces the mainstream identity addressing technology in IoT, and analyzes it in combination with the Internet addressing technology.

A. Identity Addressing Based on IP and URL

For the mainstream identity addressing method, first, according to the RFID standard system, two schemes of EPCglobal [7] and uCode [8], [43] are listed. EPCglobal is an addressing solution for EPC coding. It is proposed that the object name service (ONS) first obtains the code to be queried, and then sends the code to ONS for identity addressing, returns the address of the information server, and finally obtains the query result by accessing the address. In reality, the architecture of ONS is very similar to that of DNS, and the ONS request and response format also follows the DNS protocol. DNS is a typical addressing method based on IP and URL. However, there are some problems with this identity addressing scheme. The way in which ONS is concentrated will lead to the distrust of other systems or industries. Faced with this problem, Evdokimov *et al.* [44] proposed MONS, a modification of the existing ONS system. By backing up the copy of the root server in multiple regions and maintaining it by different independent entities, the addressing request is distributed to the local root node according to the identity of the query initiator. Balakrichenan *et al.* [45] proposed the establishment of multiple peer-to-peer root servers to manage ONS's technical solutions in a completely decentralized manner, preventing mistrust caused by power concentration. Ding *et al.* [46] designed a syntax formal decoding rule (FDR). This rule defines the addressing rules from product code to the domain name, so that the identification scheme definition is decoupled from the executable program. Song *et al.* [47] analyzed the name service challenges from the perspective of security, and proposed a smart collaborative distribution scheme for privacy enhancement to enhance user privacy in the complex environment.

For the uCode addressing system based on the uID encoding, the addressing process of the system is to read uCode from ID tag, and then the ubiquitous communicator asks ubiquitous ID center about the address of the product information service server that provides information about the uCode. The ubiquitous ID center of the query then returns the address (IP address, URL, phone number, etc.) of the product information service server to the ubiquitous communicator. A ubiquitous communicator then uses this address to access the product information service server and get information. From this, we can see that the function of the ucode parsing server is very similar to DNS. ISO/IEC is also gradually strengthening research and standardization related to the identity addressing of IoT, such as data protocol standards (ISO/IEC 15961, ISO/IEC 15962, ISO/IEC 15963, etc.), air interface standards (ISO/IEC 18000 series), and test standards (conformance test ISO/IEC 18046, performance test method ISO/ IEC 18047 corresponds to the air interface standard).

B. Identity Addressing Based on URN

From the analysis of the above identity addressing scheme, we can find that for EPCglobal and uCode, their core identity addressing functions or services are based on the traditional Internet addressing technology. In the Internet addressing, IP and URI resolution technologies, commonly used DNS technologies, are the basis for EPCglobal and uCode addressing. There is also a uniform resource name (URN)-based addressing technique. The URN [48] is developed by the Internet engineering task force (IETF). The IETF defines the syntax, possible addressing methods, and registration methods and registration procedures for the URN. The resolution service needs to rely further on the implementation of the resolution discovery system (RDS). URN is a naming scheme used to uniformly name various resources [49], [50]. The Handle system is a typical RDS system of URN. Handle system, a distributed global name service system, provides a unique identifier for information resources on the Internet [51]. The Handle system uniqueness is characterized by the fact that its information flags remain unchanged when the entity location and attributes change, and provides a good security mechanism and UTF-8 encoding. Handle's namespace consists of two parts: 1) naming authority and 2) unique local name. The Handle system consists of a global handle system (GHS) and local handle system (LHS). GHS is globally unique, and each service group can have multiple nodes. Each node can have multiple service groups. Its distributed model is embodied in the fact that the handle system defines a layered service method, and the addressing request can be addressed either through the local server or through the top-level server. The addressed data are replicated on different nodes and can be handed over to multiple servers. Each handle specifies its own manager. The addressing process is to send an addressing request carrying a handle to the Handle system on the client. When the Handle system receives the addressing request, it locates the parse request to the LHS containing the handle-related information and returns it to the client after the LHS query [52]. Compared with the traditional DNS resolution, due to the characteristics of its tree hierarchy, this resolution cannot solve its bottlenecks. Thus, these problems can be solved by a flattened addressing service architecture and the system can perform well in load balancing, and support the existing various coding methods, as well as security, confidentiality, and robustness. At the same time, the Handle system has good development prospects

in many fields, such as digital libraries and museums, digital publishing, education and scientific research, information security, and privacy protection [53].

C. Identity Addressing Based on Low Power and IPv6

However, for different network environments, such as embedded Web service networks, which are in a low power, lossy network environment, the above-mentioned traditional network protocols do not provide good support for such environment. Therefore, IPv6 over low-power wireless personal area networks (6LoWPAN), which is the name of a concluded working group in the Internet area of the IETF, puts forward a set of addressing scheme based on IPv6 [54], [55]. Luo and Sun [56] implemented the addressing process from the Internet host to the sensor node according to the proposed 6LoWPAN protocol. In terms of technology, the combination with IPv6 is also an important development direction in the field of identity modeling and addressing in the future. Most of the IoT terminal nodes interact with the network and information through IP data channels. With the rapid development of the IoT in the future, there will also be a huge demand for IP addresses. The number of addresses that IPv6 can identify is enough to provide a common and unique IP address for each IoT device.

D. Identity Addressing Based on URI and XML

Currently, different equipment manufacturers follow different proprietary agreements and IoT devices are locked in many closed ecosystems. This kind of heterogeneity hinders the development of IoT, and the Web services technology can properly alleviate this problem. IoT Web services expand traditional services from the only cyberspace to the physical space. In fact, the services of the IoT not only increase more services but also services more intelligent and convenient. Enterprises or organizations can upload their own IoT resource management platform service interface to Web services to provide services. Web services have three basic elements: 1) simple object access protocol (SOAP); 2) Web services description language (WSDL); and 3) universal description, discovery, and integration (UDDI). SOAP is a protocol specification for data exchange and a common standard in the industry. WSDL is a document written in XML that describes a Web service and provides operations or methods for that service. UDDI is a directory service that can manage Web services. With the continuous opening and sharing of the IoT, the demand for distributed Web service is more prominent. For example, distributed storage-based P2P [57] and recently popular decentralized blockchain technology can serve the IoT identity addressing technology, such as Ozyilmaz and Yurdakul [58] who proposed a blockchain-based IoT solution.

E. Intelligent Identity Addressing

Search engine is a significant technology in the Internet, which can also be used in the process of IoT addressing. This technology can support semantic understanding and search content, as well as the addressing and discovery of heterogeneous resources. We can regard the cyber entity as a Web page for daily browsing, and our information carrier also turns into a digital resource such as a Web page or a database from the original physical tag for the entity and the attribute data obtained through the sensor. In this way, we can not only rely on and learn from the good performance and implementation strategies and technologies that the search engine has developed for many years but also provide the basic platform for the IoT to move toward intelligence. In recent years, the search engine based on the IoT has also developed. For example, Ding *et al.* [59] proposed an IoT hybrid search engine technology based on time and space, value-based, and keyword-based conditions (IoT-SVK search engine), which has a good performance improvement. Liu *et al.* [60] proposed a distributed resource discovery (DRD) architecture to discover resources in M2M applications and implement interoperability between heterogeneous devices and enable resources access to resource-constrained embedded devices from the Internet. Datta *et al.* [61] proposed a framework for automatic and efficient resource discovery in the IoT. But identity addressing of IoT based on search engine also faces some challenges, such as searching for things in the IoT that require tight binding to contextual information. Lunardi *et al.* [62] proposed a context-based search method. In addition, there are other challenges, such as the data of the IoT is not the readable text data in the webpage, how to effectively migrate the data, how to solve the dynamic change of the state information of cyber entities, etc.

The search records collected by the search engine can be used to analyze the situation of the IoT identity addressing and make recommendations. For human retrieval, we can implement intelligent search based on the recommended algorithm. For machine request analysis, the integration of device services reduces network stress. The optimization results obtained through the above data analysis can further improve the knowledge/relationship graph. Regardless of whether it is a person or a machine, due to the huge size of the database and entity of the IoT, continuous query and frequent access will exert tremendous pressure on IoT services. Therefore, the above can reduce the pressure of IoT services through publish/subscribe. When a user or device subscribes to a service, the service automatically posts content to the subscriber.

Another noteworthy aspect of IoT identity addressing is the change of storage mode. A knowledge graph has been introduced in the previous section, and the introduction of the knowledge graph has brought new challenges. The traditional IoT modeling data storage format is stored in the form of a table, and both the IoT and the computer field have optimized the query and transmission process of such data formats, speeding up query efficiency. The data based on the knowledge graph are graph type data. This requires some IoT application fusion graph computing framework. Although graph computing is not a new term, the integration with the IoT industry is still in the development phase. The IoT field also has a great demand for graph computing frameworks. For example, the reasoning of the knowledge graph of large data volume and the calculation of the relationship of the IoT. Combining graph computing with IoT is a valuable research direction in the future.

TABLE II
CLASSIFICATION AND COMPARISON OF IOT IDENTITY ADDRESSING

Essential Method	Internet Addressing	IoT Identity Addressing
IP and URI	DNS	ONS
E.164 and URI	ENUM	
Low power and IPv6	N/A	6LoWPAN
URN	URN	Handle System
URI and XML	Web Service	
Intelligent Addressing	Search Engine, Semantic Understanding, Knowledge/Relationship Graph	

F. Brief Summary

Through the above introduction, we classify the IoT identity addressing and compare it with Internet addressing to form Table II.

For identity addressing, there are a large number of addressing platforms available for service, which only need to register according to the specified standards and use the interface to query and address. In order to adapt to special business scenarios to achieve effective and fast addressing, we can consider from the storage data structure, service computing power, cache, and other aspects. With the increasing demand of users, addressing service also needs to be able to understand the needs of users better. Therefore, for such addressing demand, first, the service needs to be able to understand the user's intention, obtain a specified clear addressing requirement or understand the user's description through natural language processing. The second is context analysis, through other dimensions to retrieve and enrich user environment information. The third is to aggregate the user's intention with the knowledge after index through analysis, list the solutions after matching and sorting, and finally return the solutions to the user. The scheme can also be extended and intelligent recommended, including other related and multilevel requirements of users. For the processing of dynamic data, it is suggested to change the passive mode of providing collected data to the active mode of broadcasting, which can optimize the use of resources, and the subsequent security authentication problems also need to be further considered.

Facing the identity addressing of IoT, we need to keep up with the trend of the times and continue to integrate and learn new solutions to improve the current analytical solutions. At the same time, with the continuous improvement of computing power and the continuous optimization of algorithms, the efficiency of identity addressing has been greatly improved. What is more focused now is the ability to combine multiple heterogeneous resource identity addressing, as well as the development of resource reasoning, discovery, and intelligence.

IV. IDENTITY MODELING AND ADDRESSING FRAMEWORK

Based on the above, we can find that the IoT identity has a rich development in modeling and addressing, combining specific areas and integration with the hotspot technology. This section will introduce the current mainstream IoT platform from the perspective of modeling and addressing, and propose an IoT framework with flexible applicability in the field of modeling and addressing.

Of mainstream IoT platforms, ThingWorx Platform [63] is one worth studying and focusing on. It provides users with modeling tools. In the Thing Templates, it provides the basic functions of attributes, services, events, and subscriptions used by things instances in their execution to facilitate users to model according to their business scenarios. This platform also has a good fit for the modeling field described above. The Amazon IoT platform [64] can be model-specific devices or logical entities. The JSON data form defines the version number, name and attribute of the entity, and various types of things and things are stored in the registry. The platform stores descriptions and configuration information common to all things associated with the same transaction type. It also manages and organizes transactions and security configurations through its IAM policies, and integrates commands to search for things. Bosch IoT Things [65] has similar functions to the former in terms of modeling. It adds namespace rules to ID writing, has good support in resource search, and can satisfy all kinds of requirements of query and relational operators and logical operators. The EVRYTHNG Platform [66] is a PaaS cloud platform based on IoT services. The platform is highlighted with good integration. It adds blockchain verification for EVRYTHNG operations using the Chainpoint protocol and Reactor, and integrates GS1 digital link, Sigfox, The Things network, Nest cloud, etc. IBM Washington IoT platform [67] also provides blockchain services, and devices can send data to and invoke smart contract transactions on IBM Blockchain Platform or on the open-source Hyperledger blockchain.

By combining the development of identity modeling and addressing with the characteristics of the current mainstream IoT platform, we dismantle the traditional framework, propose a scheme to reduce the coupling between functional modules, flexibly change the level, and can support the level of expansion of the identity modeling and addressing framework, as shown in Fig. 4.

A. Access Layer

The access layer is mainly used to collect events and data in the physical world, including various physical, chemical and biological data, entity characteristics and identification information, etc. Through the communication and protocol management module to deal with the different network environments and different data protocol data receiving and processing. At the same time, this layer will also monitor and record the connection and operation of the basic hardware.

B. Processing Layer

In the processing layer, it will authenticate and manage the access and control requests of the adjacent layer. At the same time, the data received by the access layer are verified and preprocessed, and the standardized data are processed according to the identity modeling method. This process removes noise data and irrelevant data from the source data set, and

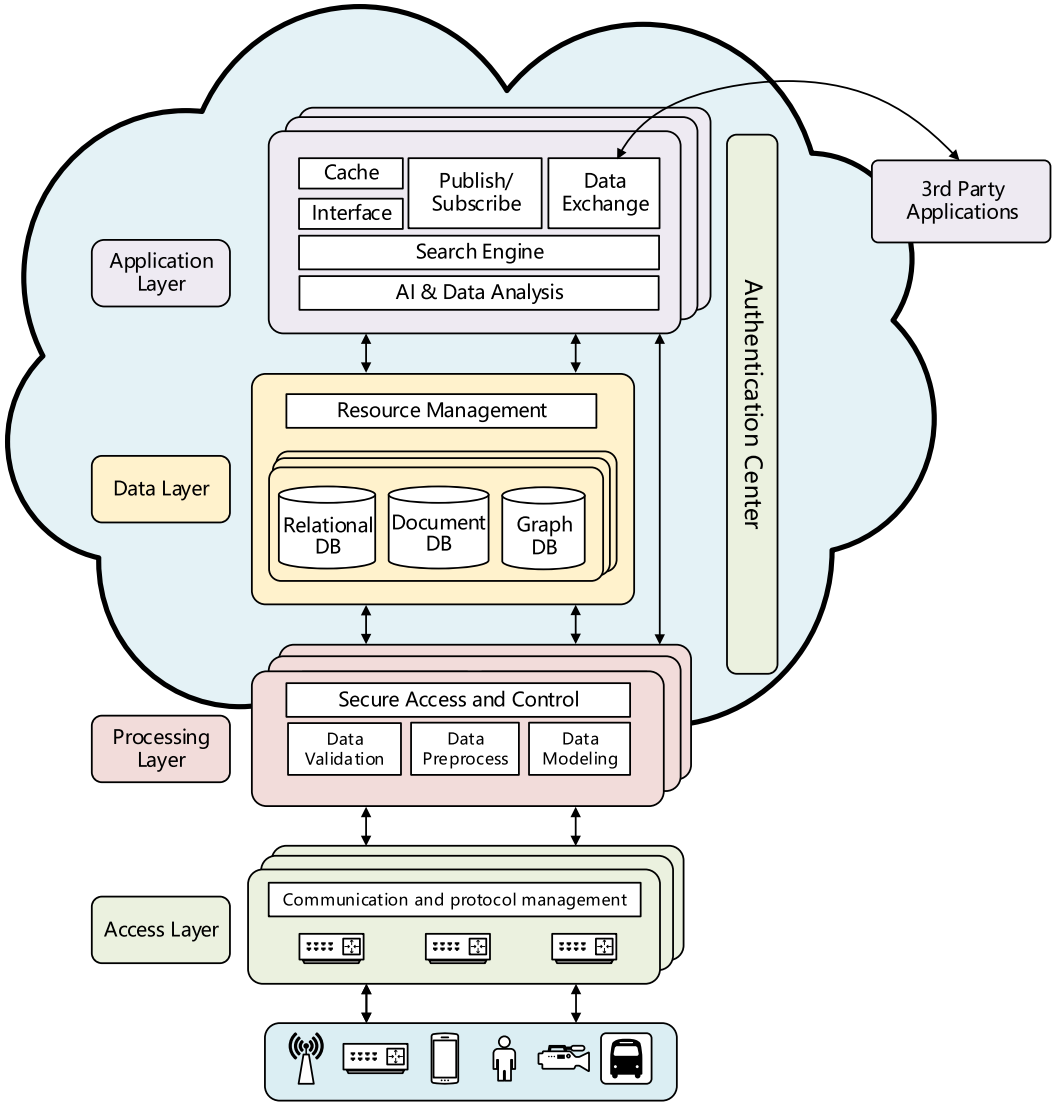

Fig. 4. Identity modeling and addressing framework.

identifies entities, relationships, events, etc. This process will also perform data reduction and data fusion processing, so as to reduce the pressure of data transmission.

C. Data Layer

The data layer is used to store data and provide a storage interface. The resource management module is responsible for the management of the layer, including search engine reverse index database, query history database, collected sensor data, and other data information. The types of databases involved in this layer are: relational databases and nonrelational databases. Nonrelational databases include document databases and graph databases. In this way, some performance optimizations can be centralized, so that IoT developers need not care about database performance.

D. Application Layer

This layer is responsible for addressing and some application modules. The AI and data analysis module will predict, cluster, analyze, and reason the data. A search engine that is used to centrally process addressing requests, and can identify traditional EPC, uCode, Handle code, etc. Based on the data exchange module, other systems can be docked with third-party applications and forwarded to the corresponding addressing platform. For the relational query and reasoning of knowledge maps, the translation of SPARQL is implemented. There is also the ability to query traditional semantic aspects, namely traditional search engines. The results of the above addressing are stored in the local cache, thereby improving query efficiency and reducing service pressure. The subscribe/publish module can be used to implement subscription and publishing of services, utilizes the Kafka technology, and is responsible for communication between layers through its message queue function snd provide some open service interfaces for developers and users to call.

E. Certification Center

Certification Center runs through the whole architecture in the cloud, and it is mainly used for authentication of access users and devices. It can effectively manage the access rights

TABLE III
FRAMEWORK PROPERTIES COMPARISON

	Traditional IoT monolith framework	Framework in this paper
Flexibility	Low	High
Scalability	Hard	Easy
Maintainability	Medium/ Bad	Good
Integration	High	Low
Reliability	Medium	High
Reusability	Bad	Good

of the request, reject and avoid illegal requests and malicious attacks, and has a better guarantee for the security of the entire architecture.

Through the analysis of many IoT platform frameworks, the platform function modules are decomposed from the perspective of identity modeling and addressing. Different from the traditional IoT framework, where the whole operation is on the cloud platform or integrated into one, the framework designed in this article splits the function hierarchically, and puts the processing layer between the cloud and the edge. Its significance is that it can not only be allocated to the edge as the way of edge computing, reduce the computational pressure of core services, reduce the transmission bandwidth but also run in the cloud as a whole with the data and application layer. In order to realize its flexibility, it needs the support of the microservice technology.

With the introduction of the microservice technology, the traditional IoT monolith framework is dismantled into a multilayer and multimodule one, from the monolith to the plurality of small modules integrated together. Multiple levels of expansion between the hierarchy and the module greatly increase the flexibility of the frame and also accord with the engineering design philosophy of high cohesion and low coupling.

Fan and Ma [68] proposed the migration method from individual services to microservice, which has enhanced the technical feasibility of this framework. At the same time, we combine the advantages of the microservice framework demonstrated by Dragoni *et al.* [69], Datta and Bonnet [70], Hasselbring and Steinacker [71], and Fowler and Lewis [72] and summarize the contents of Table III in combination with the traditional framework.

In [69], it indicates that the key characteristics of microservices are flexibility, modularity, and evolution. Microservice is a mainstream trend of software architecture, which realizes high maintenance and expansibility of software design and development. At the same time, microservice architecture inherits from the distributed system and SOA. Compared with monoliths, the complexity of monoliths is higher, and the internal dependence is more serious. Therefore, identity modeling and the addressing framework based on microservices will be more flexible, low integration, and easy to maintain than the traditional ones. In terms of program maintenance, update, and deployment, because each service unit of microservice is small, it is naturally suitable for containerization [73]. Therefore, it has good maintainability and flexibility. However, the demand for resources in monoliths is more complex. Developers have to compromise a "one size fits all" configuration, which leads to certain waste of resources and uneven distribution [69]. When microservices expand their architecture, developers are free to choose the language, framework, etc., that they think is the optimal implementation for each service [74]. However, the mode of monoliths will have some limitations on the technical requirements. With automated delivery pipelines and container tools, an updated version of the service can be deployed to the production environment in seconds [75]. In the face of some service malfunctions and problems, the malfunctions of microservices will not lead to the integrity of the system, so compared with the monoliths, it has better reliability. But microservices have one more hidden danger of communication malfunctions between microservices units than monoliths.

V. OPEN ISSUES AND CHALLENGES

A. Ease-to-Use, Semantic, Exchangeability, and Selective Sensing in Modeling

For the future development trend and challenges of the identity modeling field, we summarized the following aspects.

1) Ease-to-Use: Ease-to-use is to get data and information from the traditional data carrier and gradually pay attention to the characteristics of the entity itself. For example, in the traditional way of payment, people consume through credit card, and personal identity information is stored on the basis of credit card, while in the current payment by the scanning code, personal identity information is extracted from the entity data carrier to realize convenient service.

2) Semantic: With the continuous development of intelligence, the traditional identity modeling method has some limitations from the data representation, which makes the machine unable to better "understand" the data. In the future, the identity modeling method based on OWL will continue to develop, and with the continuous enrichment of the collection data types and the continuous progress of the computer semantic understanding, the identity modeling method will also make further development toward semantics.

3) Exchangeability: With the continuous development and maturity of the IoT technology, the development of IoT shows the phenomenon of separation between technical standards and services. Different modeling and coding methods may be used between different IoT systems, which may lead to difficulties in sharing and data exchange. Identity modeling methods also need to consider how to share and connect data more easily. The first is to build an information exchange platform, and a third-party organization will regulate and standardize the data format. For example, NIEM solves the problem of information exchange between different data formats. Another approach is unified identity modeling, which attempts to use a unique coding standard to cover all identities. This article is also an ongoing work. However, the worries of information sharing and the measures of information closure are the greater obstacles at present, because information is value, the sharing

of information may lead to the reduction of enterprise profits, the security of user information is difficult to guarantee, copyright theft and malicious tampering and illegal copying, accountability is difficult to trace. Therefore, we need to consider not only how to realize information exchange but also the problems that will be faced and need to be solved after information sharing is open. As a result, the development of IoT needs technological progress, as well as the follow-up and protection of relevant policies, regulations, and laws.

4) Selective Sensing: The development of the IoT and big data brings us more huge information flow and information resources, which is not only an opportunity but also a challenge. Limited perception ability is powerless in the face of a large number of information resources. How to better solve the conflict between this resource and service capability has become a challenge. In this regard, Ning *et al.* [76] proposed the AMiSS framework based on selective sensing, which mitigated the contradiction between universal sensing and limited sensing resources, and reduced the waste of sensing resources.

B. Intelligent, Decentralized, and Precise Service in Addressing

As for the future development trend of the identity addressing, the first is intelligence. In Section III, it is mentioned that the IoT identity addressing develops with the Internet addressing, so the IoT identity addressing will also develop in the direction of intelligence, such as intelligent addressing, service composition, and prediction. The second is decentralization, namely, decentralized computing and storage. Decentralized computing, represented by edge computing, can reduce latency, improve scalability, enhance access to information, and make business development more agile. Blockchain technology, a decentralized storage scheme, can break the fairness and authority problems brought by centralized storage and provide a storage platform with immutability, high reliability, and security.

In Section III, it is mentioned that the identity addressing of the IoT develops with the Internet addressing. Although it has a good reference for the identity addressing of the IoT, from the perspective of demand, the data scale of the IoT is larger, the types are complex, and there are highly dynamic and heterogeneous real-time changes. Therefore, there are still some differences between identity addressing of the IoT and Internet addressing, so how to better learn from the Internet addressing technology and adapt to the environment of the IoT has become a major challenge in the future. At the same time, the emergence of mass service applications and the growing demand for services show the explosive growth of applications, which makes the services provided by people not accurate and personalized. This is also a challenge we are facing and the work we are currently doing.

C. Future Network Architecture

In order to meet the changing needs of identity modeling, institutions and scholars also try to solve these problems by designing network architecture. Named data networking (NDN) funded by the National Science Foundation (NFS) is a new Internet architecture that can adapt to the current content acquisition mode naturally. As a future network architecture project, it replaces the TCP/IP communication mode network architecture with a content-centric network (CCN) architecture [77]. With a new naming scheme similar to URI, the name of data will be the core of key functions, such as routing, forwarding, security, and content delivery. Therefore, NDN network architecture is closely related to identity modeling and identity addressing, and can provide good support. In NDN, packet forwarding decision depends on the lookup operation of variable length hierarchical names rather than fixed-length. Therefore, Quan *et al.* [78] proposed a novel name lookup engine with adaptive prefix bloom filter (NLAPB) to improve the lookup speed effectively and avoid the shortages of Bloom filter. MobilityFirst [79] is committed to develop an efficient and scalable architecture for mobile services, which is also part of NSF's future network architecture project. The core idea of MobilityFirst is to separate name and address to achieve stronger mobile performance. The global unique identifier (GUID) framework based on MobilityFirst can identify users, devices, content, environment, etc. [80]. In addition, Zhang *et al.* [81] proposed a collaborative Internet architecture, SINET, which uses a 3-D decoupled reference model to solve the problems related to triple binding (resource/location binding, user/network binding, and control/data binding) in the current Internet. SINET provides a good opportunity to solve many challenging problems in the current Internet, such as energy saving, high-speed mobile support, and security issues.

D. Security and Privacy

Identity modeling and addressing construct the mapping from physical space to cyberspace, which can be regarded as the input and output of the IoT. The security and privacy issues around these two aspects are worthy of attention. From the perspective of data flow, we analyze the security issues involved in this process. We divide the data cycle into the following aspects: 1) collection; 2) modeling; 3) processing analysis; 4) storage; 5) access; and 6) sharing.

In the process of identity modeling, data collection is an important part. For some application scenarios, we need to encrypt the data collected by the sensing devices. However, the conflict between the limited computing power of the device and the resource consumption caused by encryption is a problem that needs to be weighed. Second, we need to protect the security of data collection, such as fake node and malicious data [82], which requires us to manage the situation of each node through access control. Third, the sensing node will also be attacked by external malicious attacks. For this reason, Dong and Liu [83] proposed robust and secure time synchronization protocol to prevent Sybil attacks. At the same time, Liu *et al.* [84] proposed enhanced the distributed low rate attack mitigating (eDLAM) mechanism to mitigate DDoS attacks. In addition, Ai *et al.* [85] proposed a smart collaborative routing protocol, geographic energy-aware routing and inspecting node (GIN), to ensure the reliability of data exchange.

In the specific process of data modeling, we need to consider which attributes are ciphertext, which can fundamentally protect the security of data and the privacy of users, such as identity information containing some privacy, and specify the value of this attribute as ciphertext in the model. Next, in the process of modeling, for some secret numbers or addresses, we need to better consider their rules to prevent the use of coding or address rules to discover these secret resources. Second, manage the authority of data analysts to prevent using the authority of positions to obtain and analyze data irrelevant to business without permission, or to conduct analysis and mining irrelevant to business objectives, leading to user privacy disclosure [86].

In the aspect of storage, we need to pay attention to the encrypted storage of data, which is the basic requirement to ensure the security and privacy. Second, do well in data disaster backup to prevent data loss. There is also data security audit to protect data permissions. At the same time, we need to pay attention to the trusted security destruction or deletion of data and access resources [82].

Identity addressing security involves a major problem in data access and sharing. First, the access rights of data and the authentication of requests should be achieved. In order to prevent the intervention of illegal users, we should adopt the effective authentication technology and the perfect authentication mechanism, and also consider the identification and processing of malicious requests. Data open sharing is the foundation and premise of data value. Data resources are shared and used across departments and domains, which inevitably leads to data being stored and used by all users. Improper measures taken by any user may lead to data leakage. This requires a strict open sharing strategy through data governance. In the process of data open sharing, the shared data and target objects are controlled according to the corresponding policies. At the same time, because different network nodes have different trust standards to prevent tampering, the transmission and computing trust between different nodes in the heterogeneous IoT is a challenging problem [87]. Data products are easy to copy and modify, so we need to protect the intellectual property rights of data products in the process of use and circulation, and prevent data products from being illegally copied, spread, and tampered [82].

VI. Conclusion

With the continuous convergence of the physical space, cyberspace, and social space, identity modeling and identity addressing in IoT are becoming increasingly significant. This article summarizes the developments of IoT identity modeling and identity addressing in recent years, analyzes the common features and advantages of various programs, and combs through the methods and ideas of identity modeling and identity addressing. Faced with such a complex and changing demand environment, this article proposes a flexible and low coupling framework to better adapt to various designs, together with both identity modeling and identity addressing modules. Through investigation and research, some development trends and problems in this field are found and discussed.

References

[1] J. Ma *et al.*, "Cybermatics: A holistic field for systematic study of cyber-enabled new worlds," *IEEE Access*, vol. 3, pp. 2270–2280, 2015.

[2] S. Dhelim *et al.*, "Cyberentity and its consistency in the cyber-physical-social-thinking hyperspace," *Comput. Elect. Eng.*, vol. 81, Jan. 2020, Art. no. 106506.

[3] S. A. Weis, "RFID (radio frequency identification): Principles and applications," *Int. J. Syst. Assurance Eng. Manag.*, vol. 2, no. 3, pp. 1–23, 2007.

[4] C. Liu and P. Albitz, *DNS and Bind*. Sebastopol, CA, USA: O'Reilly Media, pp. 16–24, 2006.

[5] P. N. Edwards, M. S. Mayernik, A. L. Batcheller, G. C. Bowker, and C. L. Borgman, "Science friction: Data, metadata, and collaboration," *Soc. Stud. Sci.*, vol. 41, no. 5, pp. 667–690, 2011.

[6] T. Berners-Lee *et al.*, "Uniform resource identifiers (URI): Generic syntax," IETF, RFC 2396, 1998.

[7] D. L. Brock, "The electronic product code (EPC)," Cambridge, MA, USA, Auto-ID Center, White Paper, pp. 1–21, 2001.

[8] N. Koshizuka and K. Sakamura, "Ubiquitous ID: Standards for ubiquitous computing and the Internet of Things," *IEEE Pervasive Comput.*, vol. 9, no. 4, pp. 98–101, Oct.–Dec. 2010.

[9] 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," *Chin. J. Electron.*, vol. 21, no. 2, pp. 209–214, 2012.

[10] H. Ning, Y. Fu, S. Hu, and H. Liu, "Tree-code modeling and addressing for non-ID physical objects in the Internet of Things," *Telecommun. Syst.*, vol. 58, no. 3, pp. 195–204, 2015.

[11] S. Kwok, O. P. Ng, A. H. Tsang, and H. Liem, "Physimetric identification (PHYSI-ID)—Applying biometric concept in physical object identification," *Comput. Ind.*, vol. 62, no. 1, pp. 32–41, 2011.

[12] R. Nithyanand, R. Sion, and J. Solis, "Poster: Making the case for intrinsic personal physical unclonable functions (IP-PUFS)," in *Proc. 18th ACM Conf. Comput. Commun. Security*, 2011, pp. 825–828.

[13] S. Dong, F. Farha, S. Cui, J. Ma, and H. Ning, "CPG-FS: A CPU performance graph based device fingerprint scheme for devices identification and authentication," in *Proc. IEEE Int. Conf. Depend. Auton. Secure Comput. Int. Conf. Pervasive Intell. Comput. Int. Conf. Cloud Big Data Comput. Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, 2019, pp. 266–270.

[14] M. Botts, G. Percivall, C. Reed, and J. Davidson, "OGC® Sensor Web enablement: Overview and high level architecture," in *Proc. Int. Conf. GeoSensor Netw.*, 2006, pp. 175–190.

[15] C. Prehofer, "Models at rest or modelling restful interfaces for the Internet of Things," in *Proc. Internet Things*, 2016, pp. 251–255.

[16] T. Berners-Lee, D. Connolly, L. A. Stein, and R. Swick. (Aug. 2000). *Tim Berners-Lee—Semantic Web by Tim Berners-Lee*. [Online]. Available: https://www.w3.org/2000/Talks/0815-daml-sweb-tbl/

[17] I. Szilagyi and P. Wira, "Ontologies and semantic Web for the Internet of Things—A survey," in *Proc. IEEE 42nd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, 2016, pp. 6949–6954.

[18] (2004). *RDF Primer*. [Online]. Available: https://www.w3.org/TR/2004/REC-rdf-primer-20040210/

[19] H. Hasemann, A. Kröller, and M. Pagel, "The Wiselib tuplestore: A modular RDF database for the Internet of Things," 2014. [Online]. Available: arXiv:1402.7228.

[20] C. Gutierrez, C. A. Hurtado, and A. Vaisman, "Introducing time into RDF," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 2, pp. 207–218, Feb. 2007.

[21] (2014). *RDF Schema 1.1*. [Online]. Available: https://www.w3.org/TR/rdf-schema/

[22] (2000). *Semantic Web—XML2000*. [Online]. Available: https://www.w3.org/2000/Talks/1206-xml2k-tbl/slide10-0.html

[23] (2012). *OWL 2 Web Ontology Language Document Overview*. [Online]. Available: https://www.w3.org/TR/owl2-overview/

[24] M. Compton *et al.*, "The SSN ontology of the W3C semantic sensor network incubator group," *J. Web Semantics*, vol. 17, pp. 25–32, Dec. 2012.

[25] (2016). *SAN (Semantic Actuator Network)*. [Online]. Available: https://www.irit.fr/recherches/MELODI/ontologies/SAN.html

[26] F. Ganz, P. Barnaghi, and F. Carrez, "Automated semantic knowledge acquisition from sensor data," *IEEE Syst. J.*, vol. 10, no. 3, pp. 1214–1225, Sep. 2014.

[27] (2019). *National Information Exchange Model (NIEM)*. [Online]. Available: https://www.niem.gov

[28] J. Yang, "Design and study of intelligent warehousing system based on RFID technology," in *Proc. IEEE Int. Conf. Intell. Transp. Big Data Smart City (ICITBS)*, 2019, pp. 393–396.

[29] R. Bonacin, O. F. Nabuco, and I. Pierozzi, "Modeling the impacts of agriculture on water resources: Semantic interoperability issues," in *Proc. IEEE 23rd Int. WETICE Conf.*, 2014, pp. 447–452.

[30] H. Ning, F. Shi, T. Zhu, Q. Li, and L. Chen, "A novel ontology consistent with acknowledged standards in smart homes," *Comput. Netw.*, vol. 148, pp. 101–107, Jan. 2019.

[31] A. B. Abkenar, S. W. Loke, and A. Zaslavsky, "IoT-enabled group activity recognition services using a modeling language approach," in *Proc. 3rd Int. Conf. Internet Things Smart Innov. Usages (IoT-SIU)*, 2018, pp. 1–6.

[32] H. Afzaal and N. A. Zafar, "Modeling of IoT-based border protection system," in *Proc. 1st Int. Conf. Latest Trends Elect. Eng. Comput. Technol. (INTELLECT)*, 2017, pp. 1–6.

[33] A. Gaur, B. Scotney, G. Parr, and S. McClean, "Smart city architecture and its applications based on IoT," *Procedia Comput. Sci.*, vol. 52, pp. 1089–1094, Jun. 2015.

[34] A. E. Khaled and S. Helal, "A framework for inter-thing relationships for programming the social IoT," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*. 2018, pp. 670–675.

[35] A. Li, X. Ye, and H. Ning, "Thing relation modeling in the Internet of Things," *IEEE Access*, vol. 5, pp. 17117–17125, 2017.

[36] A. Li, R. Wang, and L. Xu, "Shrink: A breast cancer risk assessment model based on medical social network," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2017, pp. 1189–1196.

[37] H. Ning, S. Dhelim, and N. Aung, "PersoNet: Friend recommendation system based on big-five personality traits and hybrid filtering," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 3, pp. 394–402, Jun. 2019.

[38] O. Mohammed, R. Benlamri, and S. Fong, "Building a diseases symptoms ontology for medical diagnosis: An integrative approach," in *Proc. 1st Int. Conf. Future Gener. Commun. Technol.*, 2012, pp. 104–108.

[39] T. R. Gruber, "Toward principles for the design of ontologies used for knowledge sharing?" *Int. J. Human–Comput. Stud.*, vol. 43, nos. 5–6, pp. 907–928, 1995.

[40] L. Zhang, "Ontology in the field of computer," *Inner Mongolia Sci. Technol. Economy*, vol. 31, no. 20, pp. 87–88, 2009.

[41] J. Arpirez, A. Gómez-Pérez, A. Lozano, and H. S. Pinto, "$(ONTO)^2$ agent: An ontology-based WWW broker to select ontologies," in *Proc. Workshop Appl. Ontol. PSMs*, Brighton, U.K., pp. 16–24, 1998.

[42] N. F. Noy and D. L. McGuinness, "Ontology development 101: A guide to creating your first ontology," Stanford Knowl. Syst. Lab., Stanford, CA, USA, Rep. KSL-01-05, 2001.

[43] K. Amanuma, "Product identification system based on ubiquitous ID technology," in *Proc. 8th IEEE Int. Conf. Ind. Informat.*, 2010, pp. 406–411.

[44] S. Evdokimov, B. Fabian, and O. Günther, "Multipolarity for the object naming service," in *The Internet of Things*. Heidelberg, Germany: Springer, 2008, pp. 1–18.

[45] S. Balakrichenan, A. Kin-Foo, and M. Souissi, "Qualitative evaluation of a proposed federated object naming service architecture," in *Proc. Int. Conf. Internet Things 4th Int. Conf. Cyber Phys. Soc. Comput.*, 2011, pp. 726–732.

[46] D. Ding, M. Li, and Z. Zhu, "Object naming service supporting heterogeneous object code identification for IoT system," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 1, 2018, pp. 545–554.

[47] F. Song *et al.*, "Smart collaborative distribution for privacy enhancement in moving target defense," *Inf. Sci.*, vol. 479, pp. 593–606, Apr. 2019.

[48] M. Mealling and R. Denenberg, "Report from the joint W3C/IETF URI planning interest group: Uniform resource identifiers (URIS), URLs, and uniform resource names (URNS): Clarifications and recommendations," IETF, RFC 3305, Aug. 2002.

[49] R. Moats, "URN syntax," RFC 2141, May 1997.

[50] L. Daigle, D. Van Gulik, R. Iannella, and P. Faltstrom, "URN namespace definition mechanisms," RFC 2611, June 1999.

[51] S. Sun, L. Lannom, and B. Boesch, "Handle system overview," IETF, RFC 3650, Nov. 2003.

[52] W. Mao, X. Sun, and F. Wang, "An Internet resource sign and addressing technology: Handle system," *Appl. Res. Comput.*, vol. 21, no. 5, pp. 252–254, 2004.

[53] X. Guo and X. Sun, "Development and application of handle system," *Digit. Lib. Forum*, vol. 8, no. 8, pp. 18–24, 2013.

[54] N. Kushalnagar *et al.*, "IPV6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals," IETF, RFC 4919, 2007.

[55] N. Kushalnagar and G. Montenegro, "Transmission of IPV6 packets over IEEE 802.15.4 networks," IETF, RFC 4944, 2007.

[56] B. Luo and Z. Sun, "Research on the model of a lightweight resource addressing," *Chin. J. Electron.*, vol. 24, no. 4, pp. 832–836, 2015.

[57] K. Aberer and M. Hauswirth, "An overview of peer-to-peer information systems." in *Proc. Workshop Distrib. Data Structures*, vol. 14, 2002, pp. 171–188.

[58] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based IoT with Ethereum, swarm, and LoRa: The software solution to create high availability with minimal security risks," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 28–34, Mar. 2019.

[59] Z. Ding, J. Dai, X. Gao, and Q. Yang, "A hybrid search engine framework for the Internet of Things," in *Proc. IEEE 9th Web Inf. Syst. Appl. Conf.*, 2012, pp. 57–60.

[60] M. Liu, T. Leppänen, E. Harjula, Z. Ou, M. Ylianttila, and T. Ojala, "Distributed resource discovery in the machine-to-machine applications," in *Proc. IEEE 10th Int. Conf. Mobile Ad Hoc Sensor Syst.*, 2013, pp. 411–412.

[61] S. K. Datta, R. P. F. Da Costa, and C. Bonnet, "Resource discovery in Internet of Things: Current trends and future standardization aspects," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, 2015, pp. 542–547.

[62] W. T. Lunardi, E. de Matos, R. Tiburski, L. A. Amaral, S. Marczak, and F. Hessel, "Context-based search engine for industrial IoT: Discovery, search, selection, and usage of devices," in *Proc. IEEE 20th Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2015, pp. 1–8.

[63] (2019). *ThingWorx Platform*. [Online]. Available: http://support.ptc.com/help/thingworx_hc/thingworx_8_hc/en/

[64] (2019). *Amazon IoT Platform*. [Online]. Available: https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html

[65] (2019). *Bosch IoT Things*. [Online]. Available: https://things.eu-1.bosch-iot-suite.com/dokuwiki/doku.php#bosch_iot_things

[66] (2019). *EVRYTHNG Platform*. [Online]. Available: https://developers.evrythng.com/docs/

[67] (2019). *IBM Watson IoT Platform*. [Online]. Available: https://www.ibm.com/support/knowledgecenter/SSQP8H/iot/kc_welcome.html

[68] C.-Y. Fan and S.-P. Ma, "Migrating monolithic mobile application to microservice architecture: An experiment report," in *Proc. IEEE Int. Conf. AI Mobile Services (AIMS)*, 2017, pp. 109–112.

[69] N. Dragoni *et al.*, "Microservices: Yesterday, today, and tomorrow," in *Present and Ulterior Software Engineering*. Cham, Switzerland: Springer, 2017, pp. 195–216.

[70] S. K. Datta and C. Bonnet, "Next-generation, data centric and end-to-end IoT architecture based on microservices," in *Proc. IEEE Int. Conf. Consum. Electron. Asia (ICCE-Asia)*, 2018, pp. 206–212.

[71] W. Hasselbring and G. Steinacker, "Microservice architectures for scalability, agility and reliability in e-commerce," in *Proc. IEEE Int. Conf. Softw. Archit. Workshops (ICSAW)*, 2017, pp. 243–246.

[72] M. Fowler and J. Lewis. (2014). *Microservices. ThoughtWorks*. [Online]. Available: http://martinfowler.com/articles/microservices.html

[73] F. Montesi, *Choreographic Programming*, IT-Universitetet i København, Copenhagen, Denmark, 2014.

[74] M. Gabbrielli, S. Giallorenzo, C. Guidi, J. Mauro, and F. Montesi, "Self-reconfiguring microservices," in *Theory and Practice of Formal Methods*. Cham, Switzerland: Springer, 2016, pp. 194–210.

[75] T. Mauro. (2015). *Adopting Microservices at Netflix: Lessons for Team and Process Design*. [Online]. Available: https://www.nginx.com/blog/microservices-at-netflix-architectural-best-practices/

[76] 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 Things J.*, vol. 6, no. 6, pp. 9531–9544, Dec. 2019.

[77] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proc. ACM 5th Int. Conf. Emerg. Netw. Exp. Technol.*, 2009, pp. 1–12.

[78] W. Quan, C. Xu, J. Guan, H. Zhang, and L. A. Grieco, "Scalable name lookup with adaptive prefix bloom filter for named data networking," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 102–105, Jan. 2014.

[79] Y. Luo, J. Eymann, K. Angrishi, and A. Timm-Giel, "Mobility support for content centric networking: Case study," in *Proc. Int. Conf. Mobile Netw. Manag.*, 2011, pp. 76–89.

[80] L. Jiang, Y. Mu, and Z. Hongbo, "Research on naming and addressing technology of Internet of Things," *Chin. J. Internet Things*, vol. 2, no. 3, pp. 44–50, 2018.

[81] H. Zhang, W. Quan, H.-C. Chao, and C. Qiao, "Smart identifier network: A collaborative architecture for the future Internet," *IEEE Netw.*, vol. 30, no. 3, pp. 46–51, 2016.
[82] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Security*, 2013, pp. 663–667.
[83] W. Dong and X. Liu, "Robust and secure time-synchronization against sybil attacks for sensor networks," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1482–1491, Dec. 2015.
[84] G. Liu, W. Quan, N. Cheng, H. Zhang, and S. Yu, "Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things," *J. Netw. Comput. Appl.*, vol. 130, pp. 1–13, May 2019.
[85] Z.-Y. Ai, Y.-T. Zhou, and F. Song, "A smart collaborative routing protocol for reliable data diffusion in IoT scenarios," *Sensors*, vol. 18, no. 6, p. 1926, 2018.
[86] D. S. Terzi, R. Terzi, and S. Sagiroglu, "A survey on security and privacy issues in big data," in *Proc. IEEE 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, 2015, pp. 202–207.
[87] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Security*, 2002, pp. 41–47.

H uansheng Ning (Senior Member, IEEE) received the B.S. degree from Anhui University, Hefei, China, in 1996, and the Ph.D. degree from Beihang University, Beijing, China, in 2001.

He is currently a Professor and the Vice Dean of the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, where he is the Vice Director of the Beijing Engineering Research Center for Cyberspace Data Analysis and Applications. He is the Founder of the Cyberspace and Cybermatics International Science and Technology Cooperation Base. His current research focuses on the Internet of Things and general cyberspace.

Zhong Zhen received the B.E. degree from the School of Information and Electrical Engineering, Hebei University of Engineering, Handan, China, in 2018. He is currently pursuing the M.S. degree with the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China.

His current research interests include identity modeling and addressing and data mining.

Feifei Shi received the B.S. degree from the China University of Petroleum, Beijing, China, and the M.S. degree from the University of Science and Technology Beijing, Beijing, where she is currently pursuing the Ph.D. degree with the School of Computer and Communication Engineering.

Her current research interests include Internet of Things and artificial intelligence.

Mahmoud Daneshmand (Life Senior Member, IEEE) received the B.S. and M.S. degrees in mathematics from the University of Tehran, Tehran, Iran, and the M.S. and Ph.D. degrees in statistics from the University of California at Berkeley, Berkeley, CA, USA.

He is currently an Industry Professor with the Department of Business Intelligence and Analytics as well as the Department of Computer Science, Stevens Institute of Technology, Hoboken, NJ, USA. He has more than 35 years of industry and university experience as: a Professor, a Researcher, an Assistant Chief Scientist, the Executive Director, the Distinguished Member of Technical Staff, the Technology Leader, the Chairman of Department, and the Dean of School with: Bell Laboratories, Murray Hill, NJ, USA; AT&T Shannon Labs-Research, Florham Park, NJ, USA; the University of California at Berkeley; the University of Texas, Austin, TX, USA; the Sharif University of Technology, Tehran, Iran; the University of Tehran, Tehran; New York University, New York, NY, USA; and the Stevens Institute of Technology. He has published more than 150 journals and conference papers; authored/coauthored three books. He is well recognized within the academia and industry and holds key leadership roles in IEEE journal publications, conferences, Industry–IEEE Partnership, and IEEE Future Direction Initiatives.

Dr. Daneshmand is the Co-Founder and the Chair of the Steering Committee of the IEEE INTERNET OF THINGS JOURNAL; a member of the Steering Committee of the IEEE TRANSACTION ON BIG DATA; a Guest Editor of several IEEE publications; the Co-Founder of the IEEE Big Data Initiative; and has served as the general chair, the keynote chair, the panel chair, and the technical program chair of many IEEE major conferences. He has given several Keynote speeches in IEEE as well as international conferences. He is an expert on Big Data Analytics with extensive industry experience including with the Bell Laboratories as well as the Info Lab of the AT&T Shannon Labs-Research.