Received July 8, 2019, accepted July 22, 2019, date of publication July 25, 2019, date of current version August 7, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2931365

Modeling Data, Information and Knowledge for Security Protection of Hybrid IoT and Edge Resources

YUCONG DUAN[1], (Senior Member, IEEE), XIAOBING SUN[2], (Senior Member, IEEE), HAOYANG CHE[3], CHUNJIE CAO[1], (Member, IEEE), ZHAO LI[4], AND XIAOXIAN YANG[5]

[1]College of Information Science and Technology, Hainan University, Haikou 570228, China
[2]School of Information Engineering, Yangzhou University, Yangzhou 225009, China
[3]Data Intelligence Center, Auto-Smart Inc., Beijing 100086, China
[4]Alibaba Group, Hangzhou, China
[5]School of Computer and Information Engineering, Shanghai Polytechnic University, Shanghai 310099, China

Corresponding author: Xiaoxian Yang (xxyang@sspu.edu.cn)

This work was supported in part by the NSFC under Grant 61662021 and Grant 61363007, and in part by the CERNET Innovation Project under Grant NGII20180607.

ABSTRACT Currently, with the growth of the Internet of Things devices and the emergence of massive edge resources, security protection content has not only empowered IoT devices with the accumulation of networked computing and storage as a flexible whole but also enabled storing, transferring and processing DIKW (data, information, knowledge, and wisdom) content at the edge of the network from multiple devices in a mobile manner. However, understanding various DIKW content or resources poses a conceptual challenge in unifying the semantics of the core concepts as a starting point. Through building metamodels of the DIKW framework, we propose to cognitively formalize the semantics of the key elements of the DIKW in a conceptual process. The formalization centers on modeling the perceived world only by relationships or semantics as the prime atomic comprising elements. Based on this cognitive world model, we reveal the difference between relationships and entities during the conceptualization process as a foundation for distinguishing data and information. Thereafter, we show the initial case for using this formalization to construct security protection solutions for edge computing scenarios centering on type conversions among typed resources formalized through our proposed formalization of the DIKW.

INDEX TERMS Knowledge graph, security protection, typed resources, edge computing.

I. INTRODUCTION

With the rapid growth of the application of various IoT (Internet of Things) [1] devices and the emergence of massive available edge resources [2]–[7], the content of security and privacy protection has increasingly empowered IoT [6], [8] devices with the accumulation of networked computing [9]–[12], resource transfer and resource storage in an integrated and flexible manner [13]. This tendency has also unprecedently enabled collection, storing, transferring, processing, transformation and utilization of DIKW (data, information, knowledge, wisdom) [14], [15] content at the edge of the network from multiple sources. The emergence of new usage requests on the accumulated content from multiple sources of various integrated, especially mobile [16], [17], devices at the edge has introduced new security challenges [18]–[20]. Security protection [42], especially of implicit content [21], [22] from multiple mobile sources in the edge, poses new challenges [23], [24] to the collection, identification, customization of protection strategies, and resource modeling of data. However, understanding the various DIKW content or resources [25] poses, at first, a conceptual challenge to its unification and the semantics of the core concepts as a starting point for subsequent resource modeling and solutions.

Through building metamodels of the DIKW framework, we propose to cognitively and constructively formalize the semantics of key elements of DIKW resources in a conceptual

The associate editor coordinating the review of this manuscript and approving it for publication was Honghao Gao.

process. The formalization focuses on the ideology of modeling the perceived world as only as relationships or semantics as the prime atomic comprising elements. We proposed this relationship-dominating expression perspective of semantics as a model of relationship-defined everything of semantics (RDXS) [26] where the semantics of concepts are evaluated from the origin of existing semantics. We proposed a conceptual formalization framework [27], [31] and theorems for existence-level semantic evaluation and reasoning to automate processing in what we call existence computation [26]. Based on this cognitive world model, we revealed the difference between concepts such as relationships and entities during the conceptualization process as a conceptual foundation to distinguish the semantics of data [28], [29] and information and knowledge. Based on this formalization of the related concepts, we proposed modeling scenarios of security protection centering resource type transitions in graph [55] forms of data graphs, information graphs and knowledge graphs [2], [30], [32]. Thereafter, we showed the initial cases of security protection in formalized scenarios for edge computing scenarios centering on type conversions among typed resources formalized through our proposed formalization of DIKW. We focused on modeling the security and privacy content [33], [34] and relationships of a smart city's multiple edge sources by classifying them as typed resources [35] of types of data, information and knowledge in our DIKW architecture, and modeling and designing resource security protection as compositions [36] of data level security, information level security, and knowledge level security. For example, a piece of content might exist explicitly as a piece of data or a set of data [37] in a data graph, or it might take the implicit [38], [39] form of being expressed as a series of relationships in an information graph. If the content is expressed in data form such as directly expressing the health condition of a human by specific indicators such as blood pressure, body weight/height, etc., the data level security protection is directed to prevent unexpected operations on target numbers. The health condition of a human can also be expressed implicitly by the walking speed, sleeping rhythm, etc., and thus, the information level protection is directed to block the probabilistic [40] links among activities and other resources for identifying [41] the speed and rhythms from the source. Thereafter, we propose protection solutions for security aspects, including resource integrity, resource confidentiality and resource availability, to support security protection for administering the city and for the citizens. We propose to protect security resources by transforming them into other typed resources in DIKW graphs, which requires considerably more resources to be evaluated in terms of computation, storage and communication in DIKW graphs. Our proposed security protection can be implemented with interactive cost-driven [43] strategies, which maximizes the benefits of stakeholders and minimizes the cost [44], [45] of stakeholders by precisely matching the expected protection degree in terms of implementation and budget plan of protection investment from global business goals on the stakeholder side. In general, we present a metamodel of typed DIKW resources and a type transformation-based value-driven resource protection approach.

The rest of this paper is organized as follows. Section 2 illustrates related work. Section 3 presents the meta-modeling and formalization of DIKW graphs. Section 4 shows the transformation mechanism of typed resources. Section 5 states the protection for aspects of security, including integrity, confidentiality and availability. Section 6 shows the simulation. We conclude in Section 7.

II. RELATED WORK

With the extensive application and rapid development of the IoT, big data and the 5G network architecture, the considerable data generated by edge equipment of smart cities and the real-time service requirements are far beyond the capacity of the traditional cloud computing model [46]. Edge computing can offload some storage and computational tasks from cloud data centers to the edge of the network, which could raise many challenges related to security and security concerns. In particular, data security protection is the most important service [2] in edge computing.

Most of the work on security preservation assumes that the data are a single table with attribute information for each of the entries [47]. However, real-world data often exist with more complexity. Real-world data are often relational, represented as multi-graphs and can exhibit rich dependencies between entities. The challenge of anonymizing graph data lies in understanding these dependencies and removing sensitive information, which can be inferred by direct or indirect means [20]. Even in single-table data, removing identifying information such as social security numbers is not enough to preserve the security of individuals represented in the data [48]. While it is possible to represent the nodes of a graph in a single table if the nodes have the same type, it is not clear how to do this when the nodes exhibit relationships and when there are nodes of different types. Miklau et al. defined k-candidate anonymity for graph data based on the degrees of the nodes in the neighborhoods of the nodes to be anonymized [49]. Zheleva proposed preserving the security of sensitive relationships in graph data [20]. Hundepool et al. proposed making useful inferences from groups while preserving the security of individuals who contributed their data [50]. Danezis et al. proposed protecting security through designing models [51]. They illustrated that security is also protected through policy and law. Eberle and Holder [52] presented an approach for discovering structural anomalies in graph-based data. Soria-Comas and Domingo-Ferrer [48] presented the idea that security degree is proportional to the exposure of the degree of linkability, which is compatible with a security model. McSherry [53] proposed focusing on sequential composition and parallel composition in composability properties. Our proposed approach to model security targets as integrity, confidentiality and availability thereafter protects target security from unwanted secondary use [54] through type-level transformation in the DIKW architecture.

Knowledge identification [57] and representation is a critical topic in AI [58]. Most embedding methods merely concentrate on the triple fitting and ignore the explicit semantic expression, leading to an uninterpretable representation form [59], [60]. Traditional embedding methods not only degrade performance but also restrict many potential applications. Chein and Mugnier [61] proposed a semantic representation method for a knowledge graph that imposes a two-level hierarchical generative process that extracts aspects and locally assigns specific categories. Mugnier [62] proposed using structural and textual encoding technology to represent a knowledge graph. Sowa [63] proposed representing knowledge in logical, philosophical, and computational foundations. Chen et al. proposed visualization of data information and knowledge [64]. We propose to protect security resources by classifying them into data, information and knowledge in a three-tier architecture consisting of a data graph, an information graph and a knowledge graph.

The dynamic reconstruction of computation and storage resources not only improves the utilization of resources but also simplifies management. Some of the workloads that use common resource computing and storage technologies can handle the current cloud system to avoid saturated clouds [65]. Shao *et al.* [66] described a payment as users use a resource security provision approach based on data graphs, information graphs and knowledge graphs. Following the ideology of value-driven design, Duan *et al.* [25] proposed a systemic formalization for using data, information and knowledge graphs for cost-effective [67] optimization purposes [68], [69]. Song *et al.* [13] argued that it is necessary to consume bandwidth to transmit resources between nodes in the Internet of Things, which aims to obtain storage and computation resources from other nodes to satisfy user demands. We protect target security resources with a cost-driven interactive method, which maximizes the benefit of stakeholders while minimizing the cost for security protection.

III. METAMODELING AND FORMALIZATION OF THE DIKW FRAMEWORK

Through extending our previous work on an empirical study of DIKW [14], [70], we proposed the following formalization of the DIKW framework, which focuses on a conceptualization process with a cognitively designed explanation to reveal the semantics of the core concepts and their extensions in our proposed expression model of relationship-defined everything of semantics.

A. GENERAL BACKGROUND OF THE PERCEIVED WORLD

We proposed the improved UML metamodel of data, information, knowledge and wisdom framework [71], as shown in Fig. 1. The modeling centers on the concepts of "human" and "existence", which we decomposed as objective existence and conceptually acknowledged existence that might be subjective. We added the confirmation of nonexistence as a form of confirmed existence because it has the deterministic semantic.

$\text{existence}_{confirmed}$
$::=<(\text{existence}_{objective}, \text{existence}_{conceptual})_{positive},$
$\text{nonexistence}_{confirmed}>$

The perceived real world, which contains the perceived objective real world, comprises content related to objective existence and aggregates conceptual existence. The objective existence matches perceived objective "True/False", while the conceptual existence can be bundled into a subjective evaluation of "Yes/No" [72], which is evaluated as conforming to. Content bundled to conceptual existence can be imaginary or incorrectly proposed content. The meaning of "Null" does not contain the subjective case of confirmation of not objectively guaranteed "No". Confirmed inconsistency automatically leads to a denial of the existence of a previously confirmed existence. The null here does not refer to the concept of empty because empty can refer to the situation of a thing is not known by a stakeholder but actually exists.

$\text{existence}_{objective}$
$::=\text{confirmation}_{objective}<\text{True, False}>$
$\text{existence}_{conceptual}$
$::=\text{confirmation}_{subjective}<\text{Yes, No}>$
$\text{nonexistence}_{confirmed}$
$::=\text{confirmation}<\text{Null, Inconsist}_{objective})>$
Null
$::=\text{False}(\text{existence}_{objective}(\text{True}))$
$::=\text{existence}_{objective}(\text{False})$

The perceived world, instead of the objective real world, lays the foundation of observation-related material and processing by humans. We propose that semantics are expressed or perceived meanings of things by humans. Intuitively, it is easy to perceive that semantics comprising both relationships and entities while confirming the intent of a human. However, if we reason recursively, it is difficult to intuitively prioritize the concepts of relationship and entity in terms of which concept is more fundamental than the other. We perceive that concept is a categorization and an express form of shared semantics by stakeholders. Both data and information can be classified as concepts as long as they go through the process of conceptualization. In general, semantics are expressed as relationships that are associated with humans among various existing conceptual content. A purpose is a semantic or relationship that has an implicit or explicit end or target or intent associated with a specific human. Value can be measured in addition to a human purpose in contrast to other choices that are relatively correspondingly based on the prejudice of difference and frequency of occurrence of the sameness in terms of quality or quantity.

semantic
$::=(\text{relationship}_{concepts} \mid \text{association}_{human(Purpose)})$
purpose_{human}
$::=\text{relationship}\ (\text{intention}_{stakeholder}, \text{relationship}_{concepts})$
$::=\text{semantic}_{human(goal)}$
value value

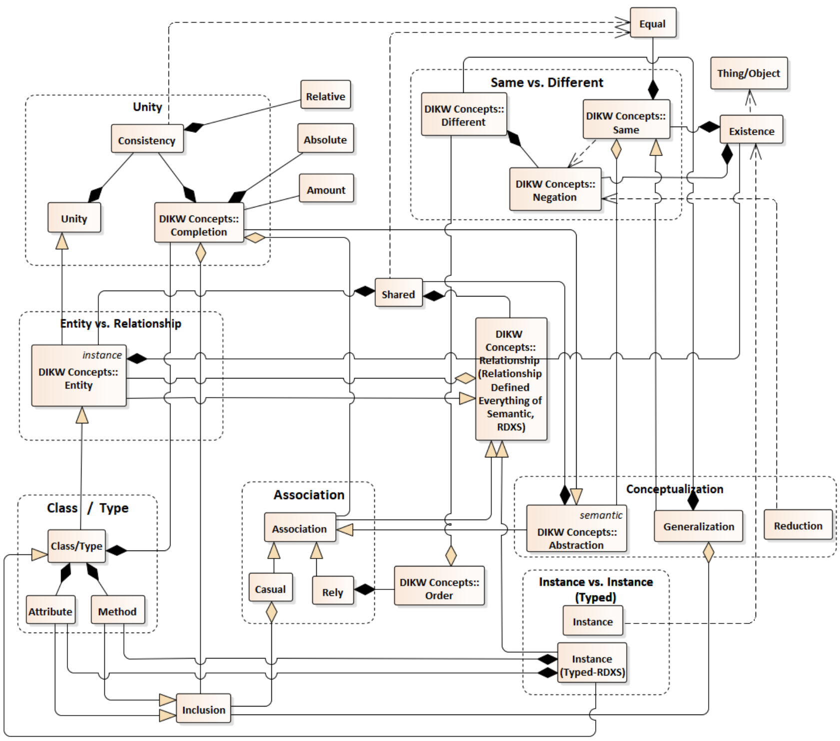


FIGURE 1. UML metamodel of same vs. different towards conceptualization of DIKW.

$::=<difference_{purpose}, sameness_{purpose}>_{relative}$
$::=relative <quality_{directed(difference)}, quantity_{frequency}>$

Distinguishing between the semantics of basic concepts of data and information demands the revelation of the hidden implicitly related conceptualization process of corresponding concepts from the atomic concepts that have clearly defined semantics [73].

B. "ENTITY VS. RELATIONSHIP" IN A PERCEIVED WORLD

According to our formalization of the difference between data vs. information, we consider the traditional problem of distinguishing between "entity vs. relationship" [74]. Through exhibition of the conceptual process of both entity and relationship, we reveal that entity is a unity that matches an individual or independent or self-complete instance that does not refer to more than one identification of existence semantic, mostly in the form of conceptual existence. Relationship is actually more fundamental than entity following the clause that everything in the perceived world is bundled with at least a purpose at the time of accomplishing the cognitive identification process. The perceived world comprises solely conceptual relationships or both implicit and explicit semantics. We propose that the relationship is the prime and solely atomic element or content of cognition. The perceived world or cognition is fully based on relationships or defined by relationships as long as the semantic is traced back to existence-level semantic evaluation. Therefore, entity as a perceived element in a perceived world is composed of atomic-level elements of relationships. In this purely constructed perceived world of relationships, every relationship is connected without exception. Relationships mutually define each other's meanings. The conversion from relationship to entity is implemented through the abstraction process, which summarizes the commonalities of relationships to form a scope as the boundary of an independent identification that can be assumed to represent an unlimited number of instances. The difference between explicit and implicit semantics is based on mismatching the relationship to entity expressions as source and target sides of expressions.

PerceivedWorld
$::=<purpose_{human} \mid relationship_{relationship} \mid semantic_{<explicit,implicit>}>$
$::=identification<relationship>$
$explicit_{<entity>}$
$::=identification_{<entity>}$
$explicit_{<relationship>}$
$::=identification_{<relationship>}$
$implicit_{<entity>}$
$::=identification_{<relationship>}$
$implicit_{<relationship>}$
$::=identification_{<entity>}$
relationship relationship
$::=<relationship>_{mutually}$
$::=<relationship>_{<relationship>}$
entity
$::=Unity(Unique(existence_{conceptual}))$
$::=<relationship>_{abstraction(completeness)}$

C. EVALUATION IN A PERCEIVED WORLD

To support deeper semantic formalization on this formalized perceived world, we propose using the conceptual difference of "same vs. different" as the foundation for further conceptualization towards extracting the formal semantic of extended concepts. Identification of things is based on the conceptual evaluation of "sameness vs. difference". The confirmation of sameness of a thing at the stage as a result of an observation constructively relates the independent thing to existing things or concepts. An identification process always needs to settle the boundary of the identification target, which is completed by bundling the semantic of completeness of the identification activation through reasoning or human interaction. The completion of settling the conceptual boundary from unlimited or unknown can be implemented through unlimited abstraction, or reasoning, or subjectively hypothesising for unknown content.

identification

$::=<\text{evaluation}_{individual}(\text{Same vs. Different}),$ $\text{Completion}_{group<quantity,sequence>}(\text{existence}(\text{content}))>$

completion

$::=(\text{unlimited}_{abstraction} \mid \text{unknown}_{reasoning|hypothesis})$

Observation of a thing can be integrated with the evaluation of whether the thing is the same or different from existing data, information and knowledge. Then, the process functions implicitly as a content generation process to implicitly evaluate "same" or "different". The result is a piece of content that we represent by default with a specific identification representing whether the target thing or content is the same as or different from an existing labeled or recognized thing or content of one or several types of DIKW resources. We separate ID as a form of information from other information because it is basic information of the existence of the targeted thing that is justified as a piece of information because it is bundled to recognize whether its original form is the same as any existing thing. If the result of the evaluation of sameness is positive, the ID of the newThing is assigned with the ID of the existing concept. Otherwise, a new ID is created with a function of CreateID for newConcept.

$\text{identification}_{purpose(same(anyexistingThing))}(\text{newThing})$

$::=(?\text{Same}(\text{existConcept, newThing}))$

$::=\text{Same}(\text{ShareIdentification})_{existConcept,newThing},$

$!\text{Same}(\text{ShareIdentification})_{existConcept,newThing})$

The meta-expression of the concept of data demands the confirmed existence of at least a piece of the semantic of existence as a pre-requisite, existence_{pre}, and a post-requisite of the explicit cognitive identification or label of a concept, which is denoted with $\text{identification}_{pst}$.

$\text{concept}(\text{Data})_{metamodel}$

$::=<\text{existence}_{pre}, \text{identification}_{pst}>$

$::=<\text{existence}_{<True,Yes>}, \text{identification}_{explicit(label)}>$

An alternative explanation of data vs. information is a specific observed piece of data that is utilized to generate information as a result of evaluating whether it is the same as a piece of existing data through relating to existing recognized content.

$\text{conversion}_{initial(purpose(conceptualization))}(\text{data} \rightarrow \text{information})$

$::=\text{evaluation}_{purpose}(\text{data})$

$::=\text{relating}_{cognition}(\text{new(data), observed(content)})$

$::=\text{relating}(\text{new(data)}, \text{observed}_{confirmed(existence)}(\text{entity, relationship}))$

$::=\text{relating}(\text{new(data)}, \text{observed}_{RDXS}(\text{relationship}))$

$::=\text{relating}_{RDXS}(\text{new(data)}\rightarrow(\text{relationship}))$

Constructively, many superficial semantics can evolve or be built on top of the generated semantics of the evaluation of "same vs. different". The contrary/negation of sameness is labelled as "different" or difference. We propose that the concepts of "class/type" comprise the core entity and developing other entity elements through the evaluation of "is-a" relationships is an extension of the evaluation of "same vs. different". Identification of sameness by humans can map to the process of abstraction on specific scenarios to collect the commonalities or shared characteristics by omitting unrelated details of a specific purpose. Abstraction comprises conceptualization processes through collecting the same or shared elements or features for integration as a new unity.

$\text{abstraction}_{purpose}$

$::=\text{collect}(\text{same}_{purpose}(\text{thing})) \text{ AND omit}(\text{different}(\text{thing}))$

$::=\text{concept}(\text{Data})_{metamodel}(\text{thing}_{relationship\rightarrow entity},$ $\text{new}(\text{identification})_{entity})$

D. ON THE SEMANTICS OF DATA AND INFORMATION

Empirically, data represents directly observed objects by stakeholders that solely contain its shared common meaning without bundled purposes. Intuitively, data are observed directly or collected independently. Therefore, data are bundled as entities with a piece of semantic completeness. The semantic of completeness originates as an output result of content processing operations and is not related to other things or related to other purposes. In the observed world, the raw material is the observed thing. If an observation stands by itself, or the observation is a result of an isolated observation or the observation is not a preparation or input of subsequence processing, the observation is not bundled with a specific human purpose or bounded for a stakeholder purpose. Then, the thing as the result between the observation with no purpose is potential data and can be mapped through its independence semantic as a single entity.

$\text{Data}_{potential}$

$::=\text{content}_{observation(independent|abstracted)}$

$::=\text{thing}_{No(purpose)}$

Enlightened by the "schemas" [75], [76] by Kant, we propose that data are things that are isolated from any human purposes. The identification of data can be cognitively defined by the direct or indirect presence of observers/stakeholders as the source of purposes. After conceptualization of an observation of a piece of content as a piece of data, it is revealed as a thing that is observed and related successfully to existing known concepts of certain types/classes through relating to existing relationships/entities in the whole network of relationships in the general background of relationship-defined everything of semantics.

$Data_{conceptualization}$
$:=(stakeholder_{observation},$
$!<purpose_{evaluation(identification(ExistingContent))}>)$
$::=sameness_{RDXS}(existing_{RDXS}(Concept_{relationship}($
$type_{ExistingContent\ Data|Information|Knowledge})))$
$::=unification_{RDXS}(identification(existence_{observation}),$
$Type_{relationship(ExistingContent(DIKW))})$

If the observation of data does not stand by itself, or the observation is not an isolated result, or the observation is a preparation or input of subsequent processing, the observation is bundled purpose of specific stakeholders. Then, the thing as the result of the observation with a purpose is a potential piece of information.

$Information_{RDXS}$
$::=(Data \mid Information \mid Knowledge)_{<observation(False(_{isolated|independent})),association(purpose)>}$
$:=(relationship_{RDXS})_{with(purpose)}$

Empirically, information refers to the composition of data or information or an association with knowledge following or under one or more specific purposes directly or indirectly. The purposes bring concrete semantics to the composition by relating to existing relationships of existing content or background. Multiple purposes can be related to data or information to realize the conceptual transition from data type to information type through relating the target data with at least a single purpose. The conceptual deduction process from data to information can be formalized as follows:

$Information_{Data\rightarrow Information}$
$::=association_{RDXS}(source_{isolated}(data), purpose_{stakeholder})$
$:=(source_{isolated(purpose}(data), (stakeholder_{implicit}, purpose))$
$:=((!stakeholder, data), (stakeholder_{implicit}, purpose))$
$:=((!stakeholder + stakeholder_{implicit}(purpose), data),$
$(stakeholder_{implicit}, purpose))$
$:=((stakeholder_{implicit}(purpose), data), (stakeholder_{implicit},$
$purpose))$
$:=(stakeholder_{implicit}(purpose), data + purpose)$
$::=(Data + purpose_{RDXS})_{stakeholder}$
$::=Relationship_{stakeholder}(data, purpose_{RDXS})$
$Information_{RDXS}$
$::=Purpose_{RDXS}\ (data \mid information \mid knowledge)$

If the purposes of stakeholders are moved off information, information is decomposed into discrete data or information. Logically, if things are not observed but are not able to be mapped to known concepts of data, it is distinguished as an unknown thing.

However, unknown is a relationship representing a negative relationship of the observed thing with existing data. This distinction is a purpose and bundles a semantic that is represented by unknown to the observed thing/content. This process generates a piece of information/semantic of "unknown" by relating the observed thing and existing the DIKW content.

$Information(unknown)_{(new(observation(thing))}, existing($
$content_{RDXS}))$
$::=Purpose_{distinction}(thing, existing(content_{RDXS}))$
$::=association(thing_{different(RDXS)} \mid thing_{same(RDXS)})$

E. ON THE SEMANTICS OF KNOWLEDGE AND WISDOM

Empirically, knowledge-based logical reasoning or value estimation on instances roughly maps to processing activities that rely on the conformance assumptions bundled with categories [75] or sampling representatives of probabilistic modelling [20]. Knowledge reasoning relies on the complete and consistent coverage of instances under the representative types or classes corresponding to underlying instances of representing data types and information types. Through abstraction processing, commonalities of instances of relationships among instances of data and information are conceptualized and categorized into representing types or classes. The representing types or classes are assumed to completely represent all instances under the types of corresponding data or information in terms of deterministic relationships among types or classes in RDXS or probabilistic assumptions of their values. With this semantic or association of assumed complete coverage from the closed world assumption (CWA) [71] bundled with type/class, deterministic reasoning on instances under this type or class can be performed by relating the unknown or unhappened things with the semantic of negation or false. However, if the completeness of coverage cannot be assumed sufficiently, the open world assumption (OWA) [71] applies from which no negation or false based on not direct mapping to the content of existing knowledge rules can be concluded or reached through associating to existing relationships.

$reasoning_{Knowledge(Class/Type)}$
$:=(abstraction(observation(True)_{limitedAmount}$
$(content_{existing})) \rightarrow consistent_{Same(characteristics|features)}$
$(unlimited\ (content_{observation(!True)})))_{CWA}\ AND\ (SameType$
$(content_{existing}, content_{observation(!True)}))$
$::=association_{RDXS}(same(type(observation(True)$
$_{limitedAmount}(content_{existing})), content_{observation(!True)}) \rightarrow$
$Consistent_{Same(relationship)}$
$(content_{observation(True)}, content_{o}bservation(!True))_{CWA}$

Based on our reasoning modes, information can be retrieved from empty or null or not relying on the existence of data.

$Null_{CWA}$
$::=Information_{False(existence(data))}(CWA)$
$::=negation(all(known)_{RDXS})$

For wisdom, we adopt the intuition from Schopenhauer [76] in which wisdom refers to the balance between reasoning and will for optimizing towards reaching comprehensive human goals that comprise various related and usually not consistently or even conflicting developing purposes. The implementation of wisdom takes the form of decision making through trade-off among existing data, information and knowledge, where the trade-off usually demands the transitional migration of resources among seemingly different domains.

$\text{Wisdom}_{ValueDriven}$
$::=(\text{trade-off}_{<purpose>}(\text{transition}_{CWA}$, inconsistent (purpose $_{RDXS}$)), composition$_{<purpose>}(\text{transition}_{OWA}$, consistent(purpose$_{RDXS}$)))

F. MODELLING TYPED DIKW RESOURCES

We define the meaning of all things in a system description as resources (RES) of DIKW types or relationships of RDXS. We define things as covering elementary targets of observation of a human represented at a given time. From a constructive perspective, the concept of typed data of D_{DIK} lays the foundation for typed resources (TR) of TR_{DIK} in the DIKW modelling framework. We propose typed data as modeling data purely comprising multiple dimensional related types (TR) or classes, which also represent all confirmed relationships of "rules" and interconnections with other types through these relationships. We define typed resources (TR_{DIK}) as a triad, where D_{DIK} represents typed data, I_{DIK} represents typed information, and K_{DIK} represents typed knowledge.

$TR(x)_{RDXS}$
$::=$Complete(instance(resource(x)))
TR_{DIK}
$::=< D_{DIK}, I_{DIK}, K_{DIK} >_{RDXS}$

TR_{DIK} is managed in a lifecycle consisting of TR_{DIK} identification, TR_{DIK} collection, TR_{DIK} storage, TR_{DIK} transmission, TR_{DIK} operation, TR_{DIK} transformation, and TR_{DIK} disposal.

For modeling typed data, we propose a definition of complete typed data (D_{DIK}), which is completely and mutually represented and modeled by its associated or observed linked types or classes or typed data, e.g., D_{DIK} of a dog is cognitively established through associating other typed resources, basically D_{DIK}, such as $TR_{haircolor}$, TR_{health}, and TR_{gender}.

D_{DIK}
$::=< D_{DIK}, \text{association}_{<TR-DIK>} >_{RDXS}$

Therefore, every D_{DIK} by its integrity is part of the whole unity in the form of a single graph or network that comprises other D_{DIK}. In this D_{DIK} graph or network, each node as a concept mapping to an entity of data is an equal contributor evaluated in the sense that the semantic is defined in the form of a relationship in the background of the whole graph of RDXS.

The modeling of data from discrete instances or values to purely comprising types or classes lays the foundation for our definition and modeling of typed information of I_{DIK} and typed of K_{DIK}. We further refine the definition of D_{DIK} by specifying the frequency value of each comprising type or class. The frequency semantic of a class or type is created through the identification process as a result of the evaluation of "same vs. different" on one of the existing comprising types or classes of existing D_{DIK}. A frequency value denoted by TF_D is marked for each dimension of a D_{DIK}, which records the repeated time or observed occurrence of the confirmation of the sameness of a specific piece of data content of a targeted type or class.

D_{DIK}
$::=<\text{identification}_{RDXS}(\text{existing}< D_{DIK} >), TF_D >$

The probability of D_{DIK} is marked with Pr_D, which is based on TF_D through enforcing classic probabilistic conditions. The basic form of I_{DIK} represents the identification of content bundled with at least a directly or indirectly confirmed judgment of the semantic based on the evaluation of sameness on D_{DIK} with the confirmation of the difference. The referred semantics of I_{DIK} include directed or behavioral or temporal relationships on D_{DIK} or I_{DIK}.

I_{DIK}
$::=<\text{association}_{directed}(\text{identification}_{TR-DIK})>$

K_{DIK} applies the completeness semantic consistently to the graphs of TR_{DIK} as a counterpart of the abstraction process from a limited number of instances to types with unlimited coverage of instances. Deduction of K_{DIK} applies the rules and structure of type level to instance level. Induction of K_{DIK} applies instance level observation to the type level.

K_{DIK}
$:=<\text{association}(\text{Induction}(TR_{DIK} \rightarrow \text{instance}_{TR-DIK})$, Deduction $(\text{instance}_{TR-DIK} \rightarrow TR_{DIK})>$

We further specify the knowledge graph in three layers of data graph (DG_{DIK}), information graph (IG_{DIK}), and knowledge graph (KG_{DIK}).

DIKWGraph_{RDXS}
$::=< DG_{DIK}, IG_{DIK}, KG_{DIK} >_{RDXS}$
$::=\text{relationship}_{RDXS}$ DG_{DIK} is a collection of discrete elements and subgraphs expressed in the form of various data structures, including arrays, lists, stacks, trees, and graphs DG_{DIK} records the frequency of D_{DIK}. The frequency of D_{DIK} (FRE) includes association frequency (A_F) and disassociation frequency (DA_F). FRE records every sub-frequency in various dimensions of D_{DIK} as

$FRE::=<A_F, DA_F>$

A_F consists of static frequency and dynamic frequency. Static frequency includes succession frequency (S_F), inclusion frequency (IC_F), causality frequency (C_F), spatial frequency (SS_F) and temporal frequency (ST_F). SF records the number of succession relationships. IC_F records the number of inclusion relationships. C_F records the number of causality relationships. SSF records the number of static spatial trajectories. STF records the number of static temporal trajectories. Dynamic frequency includes usage frequency (U_F) and behavior frequency (B_F). U_F records the number of repeated usages, which includes addition frequency, change frequency, deletion frequency and selection frequency. B_F records the number of behaviors, which consist of repeated time trajectories and corresponding activities. Fig. 2 shows the empirical components of FRE.

IV. TRANSFORMATIONS MODES OF TR_{DIK}

A. THE FRAMEWORK OF TRANSFORMATION

Although various resources are distributed in edge devices instead of uniformly stored in the cloud [19], they are still vulnerable to various unexpected operations and

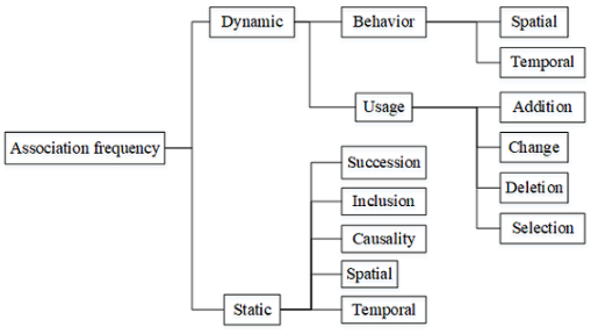


FIGURE 2. **Empirical frequency components of typed data.**

attacks. Towards designing a resource protection framework, we present a resource transformation-based protection framework of typed DIKW resources as follows.

TN::=<TN_{D-D}, TN_{D-I}, TN_{D-K}, TN_{I-D}, TN_{I-I}, TN_{I-K}, TN_{K-D}, TN_{K-I}, TN_{K-K}>. Transformations of TR_{DIK} include 9 scenarios. The expressions used are denoted as follows: R refers to the relationship, INS refers to instances of type or class, T refers to type or class, and E refers to entities that include both INS and T.

* D_{DIK} $\xrightarrow{TN_{D-D}}$ D_{DIK}: TN_{D-D} represents the resource transformation mode in which D_{DIK} is transformed to D_{DIK}. If the target D_{DIK} can be obtained from another associated D_{DIK}, we transform the target D_{DIK} into another D_{DIK} in a specific context. In the following example, E_a (INS(T_{PERSON})) is a D_{DIK}, which means a person. $E_{teacher_canteen}$INS($T_{CANTEEN}$) is a D_{DIK}, which represents an instance of canteen, and the canteen is a teacher canteen. Combining E_a (INS(T_{PERSON})) with $E_{teacher_canteen}$INS($T_{CANTEEN}$), we can infer another D_{DIK} in which the person is a teacher, which is expressed as E_a (INS($T_{TEACHER}$)). We present the process of obtaining the target D_{DIK} in which the person is a teacher as follows:
$\{D_{DIK1} = E_a\ (INS(T_{PERSON}))\}$, $D_{DIK2} = E_{teacher\_canteen}\ (INS(T_{CANTEEN}))$;
$\{D_{DIK1}\} \wedge \{D_{DIK2}\} \xrightarrow{infer} D_{DIK3} = \{E_a\ (INS\ (T_{TEACHER}))\}$.
Thus, to implement resource protection of "D_{DIK3} is a teacher", we can potentially implement the transformation from the explicit expression of D_{DIK3} to a decomposed implicit expression of the composition of D_{DIK1} and D_{DIK2} with transformation modes of TN_{D-D} as follows:
$D_{DIK3} = \{E_a\ (INS(T_{TEACHER}))\} \xrightarrow{TN_{D-D}} \{D_{DIK1}\} \wedge \{D_{DIK2}\}$
The cost of the implementation of the protection mode can be evaluated through the calculation of the basic transformation actions and the difference of the storage occupation difference before and after the transformation corresponding to the target resource.
* D_{DIK} $\xrightarrow{TN_{D-I}}$ I_{DIK}: TN_{D-I} represents the resource transformation mode in which D_{DIK} is transformed to I_{DIK}. If the target D_{DIK} can be obtained from another associated I_{DIK}, we transform the target D_{DIK} into another I_{DIK} by reorganizing D_{DIK} in real or imaginary scenarios by connecting to another D_{DIK} or I_{DIK} in terms of time or order. For example, E_a (INS(T_{PERSON})) represents a person, which is a D_{DIK}. E_{jazz} (INS(T_{CLASS})) represents an instance of a class, which is a jazz class. $R_{teach}E_a$ (INS(T_{PERSON})), E_{jazz} (INS(T_{CLASS})) represents the I_{DIK} in which a person teaches a jazz class. Thus, we obtain that the occupation of the person is a jazz dancer.
$\{I_{DIK1} = R_{teach}\{E_a\ (INS(T_{PERSON})),$
$E_{jazz}\ (INS(T_{CLASS}))\}$
$\xrightarrow{infer} \{D_{DIK1} = E_{jazz_dancer}\ (INS(T_{OCCUPATION}))\}$.
Thus, for implementing resource protection of D_{DIK3}, we can potentially implement the resource type transformation from the target D_{DIK1}, which represents it as a jazz dancer in terms of the occupation of a person into I_{DIK1} in which the person teaches jazz class with TN_{D-I} as follows:
$\{D_{DIK1} = E_{jazz_dancer}(INS(T_{OCCUPATION}))\} \xrightarrow{TN_{D-I}} \{I_{DIK1} = R_{teach}(D_{DIK1}, E_{jazz}\ (INS(T_{CLASS})))\}$.
* D_{DIK} $\xrightarrow{TN_{D-K}}$ K_{DIK}: D_{DIK} inherits semantic relationships from a type-level knowledge-base and is effectively integrated and reused by other applications. In the conversion process from D_{DIK} to K_{DIK}, if the target D_{DIK} can be obtained from other associated K_{DIK} through semantic reasoning or probability, we transform the target D_{DIK} into other K_{DIK} through linking D_{DIK} sources and semantic constraints and eliminating the redundancy and inconsistency of D_{DIK} to form K_{DIK}. For example, a person loves playing football is expressed as the K_{DIK} in which $R_{like}(E_a(INS(T_{PERSON})), E_{football}(INS(T_{GAME})))$. We can obtain the person's hobby is playing football from the K_{DIK} based on the common sense knowledge that a hobby refers to the activities that a person frequently practices or wants to practice in during a leisure period.
$\{K_{DIK1} = R_{like}\ (E_a(INS(T_{PERSON})), E_{football}\ (INS\ (T_{GAME})))\} \wedge \{T_{HOBBY} = R_{is-a}\ (E_{game}(INS(T_{ACTIVITY})), E_{like}\ (INS(T_{stable})))\}$
$\xrightarrow{infer} \{D_{DIK1} = E_{football}(INS(T_{HOBBY})))\}$.
Therefore, to implement the resource protection of D_{DIK1}, we can transform the target D_{DIK1} into K_{DIK1} with the resource transformation mode of TN_{D-K} as follows:
$\{D_{DIK1} = E_{football}(INS(T_{HOBBY}))\} \xrightarrow{TN_{D-K}} \{K_{DIK1}\}$.
* I_{DIK} $\xrightarrow{TN_{I-D}}$ D_{DIK}: TN_{I-D} represents the scenario in which I_{DIK} transforms to D_{DIK}. If the target I_{DIK} can be obtained from other associated D_{DIK}, we transform the target I_{DIK} into other D_{DIK} by transforming collections of concepts to resource instances. For example, with a high probability, we can infer that a person is a master candidate from the person's student occupation and that

the age of the person is 24 years old, which is well above the age scope of most undergraduate students:

$\{D_{DIK1} = E_{student}$ (INS($T_{OCCUPATION}$))$\} \wedge D_{DIK2} = E_{24}$ (INS(T_{AGE}))$\}$

$\underrightarrow{\text{infer}}$ $\{I_{DIK1} = R_{is}(E_a$ (INS(T_{PERSON})), E_{master} (INS(T_{DEGREE})))$\}$.

Therefore, to implement resource protection of I_{DIK1}, we can transform the explicit target I_{DIK1} into the implicit composition of D_{DIK1} and D_{DIK2} as follows:

$\{I_{DIK1} = R_{is}(E_a$ (INS(T_{PERSON})), E_{master} (INS(T_{DEGREE})))$\}$ $\underrightarrow{TN_{I-D}}$ $\{D_{DIK1}\} \wedge \{D_{DIK2}\}$.

For this conversion, there is information loss because the semantic of I_{DIK1} is probabilistically embedded in the expression of the composition of D_{DIK1} and D_{DIK2}. Therefore, in the value-driven implementation of this protection strategy, it is necessary to perform a full trade-off before adopting this strategy and continue to evaluating the quantitative gains vs. loss.

* I_{DIK} $\underrightarrow{\mathbf{TN}_{I-I}}$ I_{DIK}: TN_{I-I} represents the resource protection mode in which I_{DIK} is transformed to I_{DIK}. If the target I_{DIK} can be obtained from another associated I_{DIK}, we transform the target I_{DIK} into another I_{DIK} by connecting D_{DIK} with another D_{DIK} or I_{DIK} in a specific context and then take roles in real or imaginary scenarios to create I_{DIK}. For example, the occupation of a person is an officer, which is expressed as $E_{officer}$(INS($T_{OCCUPATION}$)). We obtain that the person is off duty at 17:00 because of the special nature of his/her work, which is expressed as:

$R_{endwork}(E_{officer}$(INS($T_{OCCUPATION}$)), $E_{17:00}$(INS (T_{TIME}))).

$\{I_{DIK1} = R_{is}(E_a$ (INS(T_{PERSON})), $E_{officer}$(INS($T_{OCCUPATION}$)))$\}$

$\underrightarrow{\text{infer}}$ $\{I_{DIK2} = R_{endwork}(E_{officer}$(INS ($T_{OCCUPATION}$)), $E_{17:00}$(INS(T_{TIME})))$\}$.

Thus, to implement resource protection of I_{DIK2}, we can transform the target I_{DIK2} into I_{DIK1} with TN_{I-I} as follows:

$\{I_{DIK2} = R_{endwork}(E_{officer}$(INS($T_{OCCUPATION}$)), $E_{17:00}$(INS(T_{TIME})))$\}$ $\underrightarrow{TN_{I-I}}$ $\{I_{DIK1}\}$.

* I_{DIK} $\underrightarrow{\mathbf{TN}_{I-K}}$ K_{DIK}: TN_{I-K} represents the scenario in which I_{DIK} transforms into K_{DIK}. If the target I_{DIK} can be obtained from another associated K_{DIK}, we transform the target I_{DIK} into another K_{DIK} by categorizing and abstracting interactive and behaviour records. For example, a girl wants to choose a hobby class. According to the K_{DIK} that girls like dancing, we infer the I_{DIK} that the girl will choose a dancing class.

$\{K_{DIK1} = R_{like}(T_{GIRL}, E_{dance}$ (INS($T_{ACTIVITY}$)))$\}$ $\underrightarrow{\text{infer}}$$\{I_{DIK1} = R_{choose}$(INS($T_{GIRL}$), E_{dance} (INS (T_{CLASS})))$\}$.

Therefore, to implement resource protection of I_{DIK1}, we transform the explicit target I_{DIK1} into K_{DIK1} with TN_{I-K} as follows:

$\{I_{DIK1} = R_{choose}$(INS(T_{GIRL}), E_{dance} (INS(T_{CLASS})))$\}$ $\underrightarrow{TN_{I-K}}$ K_{DIK1}.

* K_{DIK} $\underrightarrow{\mathbf{TN}_{K-D}}$ D_{DIK}: TN_{K-D} represents the scenario in which K_{DIK} transforms into D_{DIK}. If the target K_{DIK} can be obtained from another associated D_{DIK}, we transform the target K_{DIK} into another D_{DIK} by extracting nodes that are associated with instances in the form of attribute relationships in K_{DIK}. For example, we obtain the K_{DIK} that a rabbit likes carrots from an observation of D_{DIK1} searching for a carrot when it is hungry.

$\{R_{searchFOOD}(D_{DIK1} = E_{rabbit}$ (INS(T_{ANIMAL})), E_{carrot} (INS(T_{FOOD})))$\}$ $\underrightarrow{\text{infer}}$ $\{K_{DIK1} = R_{like}(D_{DIK1}, E_{carrot}$ (INS(T_{FOOD})))$\}$.

Thus, to implement resource protection of K_{DIK1}, we transform the target K_{DIK1} into D_{DIK1} with TN_{K-D} as follows:

$K_{DIK1} = R_{like}(D_{DIK1}, E_{carrot}$ (INS(T_{FOOD}))) $\underrightarrow{TN_{K-D}}$ D_{DIK1}.

Using an instance to represent type-level knowledge causes the reverse abstraction challenge in which multiple explanations can arise for the same instance because abstraction is based on instances of a certain quantity.

* K_{DIK} $\underrightarrow{\mathbf{TN}_{K-I}}$ I_{DIK}: TN_{K-I} represents the protection mode in which K_{DIK} transforms into I_{DIK}. If the target K_{DIK} can be obtained from another associated I_{DIK}, we transform the target K_{DIK} into another I_{DIK} through the process of knowledge searching to knowledge creation. For example, we obtain the K_{DIK1} that the hobbies of boys are usually different from the hobbies of girls according to the combination of I_{DIK1} in which boys like playing the football and the I_{DIK2} in which girls like watching Korean dramas.

$\{I_{DIK1} = R_{like}(T_{BOY}, E_{football}$ (INS(T_{GAME})))$\} \wedge$
$\{I_{DIK2} = R_{dislike}(T_{BOY}, E_{Korean}$ (INS($T_{PROGRAM}$)))$\} \wedge$
$\{I_{DIK3} = R_{dislike}(T_{Girl}, E_{football}$ (INS(T_{GAME})))$\} \wedge$
$\{I_{DIK4} = R_{like}(T_{GIRL}, E_{Korean}$ (INS($T_{PROGRAM}$)))$\}$
$\underrightarrow{\text{infer}}$ $K_{DIK1} = R_{different}(E_{girl's}$ (INS (T_{HOBBY})), $E_{boy's}$ (INS(T_{HOBBY}))).

Hence, to implement resource protection of K_{DIK1}, we can transform the target K_{DIK1} into I_{DIK1}, I_{DIK2}, I_{DIK3} and I_{DIK4} with TN_{K-I} as follows:

$K_{DIK1} = R_{different}(E_{girl's}$ (INS (T_{HOBBY})), $E_{boy's}$ (INS(T_{HOBBY}))) $\underrightarrow{TN_{I-K}}$ $\{I_{DIK1}\} \wedge \{I_{DIK2}\} \wedge \{I_{DIK3}\} \wedge \{I_{DIK4}\}$.

Or

$K_{DIK1} = R_{different}(E_{girl's}$ (INS (T_{HOBBY})), $E_{boy's}$ (INS(T_{HOBBY}))) $\underrightarrow{TN_{I-K}}$ $\{I_{DIK1}\} \wedge \{I_{DIK3}\}$.

* K_{DIK} $\underrightarrow{\mathbf{TN}_{K-K}}$ K_{DIK}: TN_{K-K} represents the scenario in which K_{DIK} transforms into K_{DIK}. If the target K_{DIK} can be obtained from another associated K_{DIK}, we transform the target K_{DIK} into another K_{DIK} through logically reasoning and mining implicit resources. For example,

we can obtain the K_{DIK2} that rabbits have a small caecum from the K_{DIK1} that rabbits like eating carrots.
$\{K_{DIK1} = R_{like}(E_{rabbit}\ (INS(T_{ANIMAL})), E_{carrot}\ (INS(T_{FOOD})))\}$
$\xrightarrow{infer} \{K_{DIK2} = R_{has\_a\_small}(T_{RABBIT}, T_{CAECUM})\}$;
Hence, to implementat resource protection of K_{DIK2}, we can transform the target K_{DIK2} into K_{DIK1} with TN_{K-K} as follows:
$\{K_{DIK2} = R_{has\_a\_small}(T_{RABBIT}, T_{CAECUM})\}$
$\xrightarrow{TN_{K-K}} K_{DIK1}$.

B. INTERACTIVE COST-DRIVEN PROTECTION FOR TR_{DIK}

Usually, target TR_{DIK} exists in more than one trajectory of subgraphs. We can obtain target TR_{DIK} directly after traversing these trajectories or inferring target TR_{DIK} with other resources in the same trajectory. According to TN, every TR_{DIK} can be replaced with another TR_{DIK} after transformation. The core of the proposed security protection is transforming target TR_{DIK} into another TR_{DIK}, which requires considerably more resources to be evaluated in terms of computation, storage [56] and communication in DIKW graphs. To minimize the cost of protection and maximize the stakeholder's benefit, we use a cost-driven interactive method to choose an optimal transformed trajectory for stakeholders. We define an interactive cost-driven protection for TR_{DIK} as CD_P. CD_P includes modules as follows:

CD_P: = (IFL(), FD(), SUM_{TN}(), SUM_{COM}(), OC()).

(i) IFL(TR_{DIK}) → Q[ifl_1, $ifl_2 \ldots ifl_n$]: IFL() refers to the function of computing the influence of each TR_{DIK}. We input different targets TR_{DIK} into IFL(). IFL() outputs influence the value of every node (V_{IFL}). Array Q records the output results of every node in descending order according to their numerical values. The calculation of V_{IFL} is as follows:

$$V_{IFL} = (deg^{+} + deg^{-})/2 \tag{1}$$

(ii) FD (Q)→ T_i: FD() is a searching function of transformed trajectories (T_i) for target TR_{DIK}. FD() conducts TR_{DIK} in the same order as TR_{DIK} storing in the array Q. For example, we traverse and determine the target D_{DIK} inferred from I_{DIK1} in IG_{DIK} or K_{DIK2} in KG_{DIK}. Therefore, we identified 2 trajectories as follows: T_1: $D_{DIK} \xrightarrow{TN_{D-I}} I_{DIK1}$ and T_2: $D_{DIK} \xrightarrow{TN_{D-K}} K_{DIK1}$.

(iii) SUM_{TN} (Q, T_i)→ $COST_{TN}$: SUM_{TN} () is a calculating function of transformed cost. The input of SUM_{TN} is each TR_{DIK} in array Q, then the transformed cost of each corresponding transformed trajectory (T_i) is calculated. $COST_{TN}$ records the results of the calculation, each of which is shown as Eq. (4). $UC_{TR_{DIKi}-TR_{DIKj}}$ is the atomically transformed cost of TR_{DIKj}. i is the number of transformed nodes in target TR_{DIK}.

$$COST_{TN} = \sum_{i=1}^{n} UC_{TR_{DIKi}-TR_{DIKj}} \tag{2}$$

(iv) SUM_{COM} (Q)→ $COST_{TOT}$: SUM_{COM} is a function for calculating the total cost of protecting typed resources ($COST_{TOT}$). $COST_{TOT}$ consists of the destroying cost (P_{DES}), the searching cost (P_{SE}) and the transforming cost ($COST_{TN}$). P_{DES} refers to the cost of destroying the links between nodes in TR_{DIK}. P_{SE} refers to the cost of searching the target TR_{DIK} in the corresponding graph. The calculation of $COST_{TOT}$ is shown as Eq. (5):

$$COST_{TOT} = \sum_{i=1}^{n} P_{DES} + \sum_{i=1}^{n} P_{SE} + COST_{TN} \tag{3}$$

(v) OC ($COST_A$, $COST_{TOT}$, $COST_P$) → Maximum ($COST_A$/$COST_P$): OC() is a function of choosing the optimal conversion plan for stakeholders. Comparing the cost of attackers ($COST_A$) with the cost of stakeholders ($COST_P$), we choose an optimal conversion plan for stakeholders to protect security resources, which maximizes the benefit of stakeholders while minimizing the $COST_P$. To obtain the optimal plan of transformation, there are three scenarios:

* ($COST_{TOT}$>$COST_A$) ∧ ($COST_P$<$COST_{TOT}$)$\xrightarrow{calculate}$ Array Q(k)→Array Q(k+1). When the total cost of transformation is larger than the cost of attackers and the cost of stakeholders, calculate the next TR_{DIK} in array Q.
* ($COST_{TOT}$>$COST_A$) ∧($COST_P$>$COST_{TOT}$) $\xrightarrow{choose}$ PL_i with min ($COST_{TOT}$). When the total cost of transformation is larger than the cost of attackers and smaller than the cost of stakeholders, choose the trajectory that has the minimum total cost.
* ($COST_{TOT} \leq COST_A$) $\xrightarrow{until}$ ($COST_{TOT}$>$COST_A$). When the total cost of transformation is smaller than or equal to the cost of attackers, calculate the next transformed trajectory until the scenario in which the total cost is larger than the cost of the attacker appears.

V. COMPONENTS OF RESOURCE SECURITY PROTECTION

With the popularity of smart devices in smart cities, current smart systems in smart cities are not competent in managing users' sensitive data, and they are causing security leakage. Edge computing can offload some storage and computational tasks from cloud data centers to the edge network, which raises many challenges related to security concerns. Sun et al. presented a comparative research analysis of the existing research work regarding the techniques used in cloud computing through data security aspects, including data integrity, confidentiality, and availability [19]. We build security in edge computing based on resource security aspects, including resource integrity, resource confidentiality and resource availability.

Security::=<INT, CONF, AVA>.

Security consists of resource integrity (INT), resource confidentiality (CONF) and resource availability (AVA). Table 1 shows the components of resource security. Resource integrity includes D_{DIK} integrity (INT_D), I_{DIK} integrity (INT_I) and K_{DIK} integrity (INT_K). Resource confidentiality includes D_{DIK} confidentiality ($CONF_D$), I_{DIK} confidentiality ($CONF_I$) and K_{DIK} confidentiality ($CONF_K$). Resource

TABLE 1. Components of security.

Type	Integrity	Confidentiality	Availability
D_{DIK}	INT_D	$CONF_D$	AVA_D
I_{DIK}	INT_I	$CONF_I$	AVA_I
K_{DIK}	INT_K	$CONF_K$	AVA_K

availability consists of D_{DIK} availability (AVA_D), I_{DIK} availability (AVA_I) and K_{DIK} availability (AVA_K).

A. RESOURCE INTEGRITY AND CORRESPONDING PROTECTION

Resource integrity is a significant concept in the security protection of resources. Resource integrity refers to protecting resources from unexpected operations such as deleting, modifying or fabricating by unauthorized attackers. We attempt to protect resource integrity in DIKW graphs to ensure that the valuable resources are not lost, changed, stolen or altered with a certain measurable degree with an explicitly accepted cost or charge for enacting the protection implementation. Resource integrity in DIKW graphs covers resource types of data, information and knowledge for which we denote the corresponding integrity with INT_D, INT_I and INT_K.

We designed a smart city monitoring system to illustrate the protection of resource integrity. The smart city monitoring system consists of a geographic location acquisition module, credit card consumption tracking module, video acquisition module and resource analysis module. We collected resources and constructed DG_{DIK}, IG_{DIK} and KG_{DIK}.

For example, the grade list of a class includes name, student number, subject and corresponding grade, which is expressed as grade_ list = INS(T_{NAME}), INS(T_{NUMBER}), INS($T_{SUBJECT}$), INS(T_{GRADE}). To ensure the resource integrity of the grade list, we classify records as corresponding D_{DIK} in DG_{DIK}:

$D_{DIK1} = \{INS\ (T_{NAME})\} \wedge D_{DIK2} = \{INS\ (T_{NUMBER})\} \wedge D_{DIK3} = \{INS\ (T_{SUBJECT})\} \wedge$

$D_{DIK4} = \{INS\ (T_{GRADE})\} \xrightarrow{constitute} D_{DIK} = \{D_{DIK1}, D_{DIK2}, D_{DIK3}, D_{DIK4}\}$.

We classify the order of the grade and student's name of the corresponding grade as I_{DIK}:

$I_{DIK1} = Rdescending\{T_{NAME}, T_{GRADE}\}, I_{DIK2} = R_{is}\{T_{NAME}, T_{GRADE}\}$.

INF_D refers to protecting D_{DIK} from unauthorized deliberate destroying operations when $D_{DIK2} = \{No.2\}$ in the grade list is deleted. Meanwhile, the corresponding D_{DIK} of D_{DIK2} is modified as $D_{DIK1} = \{Amy\}$. We obtain D_{DIK1} from D_{DIK4} that is the student's grade, and I_{DIK2} is the corresponding name of the grade.

$\{D_{DIK4} = 60\} \wedge \{I_{DIK2} = R_{is}(Amy, 60)\} \xrightarrow{infer} D_{DIK1} = \{Amy\}$.

D_{DIK1} is absent, and D_{DIK1} corresponds to D_{DIK2}, transform D_{DIK2} as $\{D_{DIK2}\} \xrightarrow{TN_{D-D}} \{D_{DIK1}\}$. We protect D_{DIK1} and D_{DIK2} to ensure the INT_D.

INT_I refers to protecting I_{DIK} from unauthorized deliberate deleting, modifying or fabricating. If target I_{DIK1} is fabricated, based on TN with $\{I_{DIK1}\} \xrightarrow{TN_{I-D}} \{D_{DIK}\}$, we cannot obtain the I_{DIK1} from $D_{DIK} = \{D_{DIK1}, D_{DIK2}, D_{DIK3}, D_{DIK4}\}$ with K_{DIK} in which the rules of ascending order, descending order, or disorder are $\{D_{DIK}\} \xrightarrow{K_{DIK}} \{I_{DIK1}\}$. We protect the INT_I of I_{DIK1} by deleting it.

Algorithm 1 shows the process for protecting the resource integrity. In DIKW graphs, security resources are associated with another TR_{DIK}. Hence, INT is achieved by establishing a mutual check between TR_{DIK} with a transformation mechanism.

Algorithm 1 Protecting Resources From Unauthorized Destroying Operations

Input: User's ID ed_i and corresponding operations $OP = \{op_1, op_2 \ldots op_n\}$;
Output: initial $ID_{DIK} = \{dx_1, dx_2 \ldots dx_k \ldots dx_n\}$;
1: import accessible $U_{ID} = \{id_1, id_2 \ldots id_n\} \in D_{DIK}$;
2: **for** ($ed_i \notin U_{ID}$) **do**
3: **if** ((sum(dx) = n) $\xrightarrow{op_i}$ (sum(dx) $\neq$ n)) //deleted by unauthorized users
4: determine deleted element as dx_k;
5: search $\{TR_{DIK} | (dx_k \vdash TR_{DIK})\}$;
6: **else if** (($dx_k' = dx_k$) $\xrightarrow{op_i}$ ($dx_k' \neq dx_k$)) // modified by unauthorized users
7: search $\{TR_{DIK} | (dx_k \vdash TR_{DIK})\}$;
8: **else if** (($dx_k \vdash TR_{DIK}$) $\xrightarrow{op_i}$ ($dx_k \nvdash TR_{DIK}$)) // fabricated by unauthorized users
9: delete dx_k;
10: $(D_{DIK} \xrightarrow{TN_{D-D}} dx_k) \wedge (I_{DIK} \xrightarrow{TN_{I-D}} dx_k) \wedge (K_{DIK} \xrightarrow{TN_{K-D}} dx_k)$;
11: merge dx_k in ID_{DIK};
12: return ID_{DIK};
13: **end for**;

B. RESOURCE CONFIDENTIALITY AND CORRESPONDING PROTECTION

Resource confidentiality is critical for users to store their security resources in the edge cloud. Resource confidentiality refers to ensuring edge cloud reliability and trustworthiness with strategies of authentication and access control. Simple encryption has a key management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization [19]. We solve resource confidentiality including $CONF_D$, $CONF_I$ and $CONF_K$ in DIKW graphs. Because D_{DIK} in DG_{DIK} is associated with I_{DIK} and K_{DIK}, once DG_{DIK} records the authentication of a user, the record updates in both IG_{DIK} and KG_{DIK}, and it is difficult to change the record.

Algorithm 2 gives the authentication and access control strategy, which prohibits unauthorized users from accessing valuable resources. After inputting user ID and corresponding operations, ID and operations are matched with available ID in DG_{DIK} and appropriate operations in IG_{DIK}. When the return is p = 1, the user is prohibited.

Algorithm 2 Authentication and Access Control Strategy

Input: User's ID ed_i and corresponding operations $OP = \{op_1, op_2 \ldots op_n\}$;
Output: Prohibit the user ($p = 1$) or not ($p = 0$);
import accessible $U_{ID} = \{id_1, id_2 \ldots id_n\} \in D_{DIK}$;
import allowable $OP_C = \{cp_1, cp_2 \ldots cp_n\} \in I_{DIK}$;
for ($ed_i \in U_{ID}$) **do**
  if ($op_i \in OP_C$) $p = 0$;
  else $p = 1$;
return p;
end for;

C. RESOURCE AVAILABILITY AND CORRESPONDING PROTECTION

Resource availability is very important for users to estimate and evaluate the possibility of recovery and verification of their resources by techniques rather than depending only on the credit guarantee of the cloud service provider. Resource availability protection helps users not only ensure the confidence of recovering security resources but also protect sensitive security resources from unexpected access, access blocking and modification operations. Recovery degree can be used to help users quantitatively know the availability of D_{DIK} and measure the result of using the D_{DIK}. The degree of re-coverage is a critical indicator of resource availability. The recovery degree is relative to the ratio of D_{DIK} after recovering (dx_i') and initial D_{DIK} (dx_i) without destroying. The calculation of recovery degree is shown as Eq. (6), DEG_R represents the recovery degree where n refers to the number of surveyed cases.

$$DEG_R = \frac{1}{n}\sum_{i=1}^{n}[\frac{(dx_i')}{(dx_i)}] \tag{4}$$

Resource availability includes AVA_D, AVA_I and AVA_K. AVA_D and AVA_I are achieved in the proposed DIKW framework by transforming target D_{DIK} or I_{DIK} to another TR_{DIK}. Algorithm 3 shows the process of recovering D_{DIK}, which is destroyed by inappropriate operations and sends feedback on the recovery degree to users.

For example, the grade list of a class includes name, student number, subject and corresponding grade, which is expressed as grade_ list = {INS(T_{NAME}), INS(T_{NUMBER}), INS($T_{SUBJECT}$), INS(T_{GRADE})}. To protect resource availability of the grade list, we classify records as corresponding D_{DIK} in DG_{DIK}:

D_{DIK1} = {INS (T_{NAME})} ∧ D_{DIK2} = {INS (T_{NUMBER})} ∧D_{DIK3} = {INS ($T_{SUBJECT}$)}∧

D_{DIK4} = {INS (T_{GRADE})} $\xrightarrow{\text{comprise}}$ D_{DIK} = {D_{DIK1}, D_{DIK2}, D_{DIK3}, D_{DIK4}}.

We classify the order of the grade and the score of each part in the paper as I_{DIK}:

$I_{DIK1} = R_{acsending}T_{NAME}, T_{GRADE}$, $I_{DIK2} = R_{is}${INS (T_{PART}), INS(T_{SCORE})}.

AVA_D refers to recovering D_{DIK} from inappropriate insertion, deletion, update and selection. Taking D_{DIK4} as an example, according to the proposed TN, we protect the AVA_D of D_{DIK4} with {D_{DIK4}} $\xrightarrow{TN_{D-I}}$ {I_{DIK2}}. If target D_{DIK4} is important, we obtain the D_{DIK4} from I_{DIK} in which the score of each part with K_{DIK} and the sum of each part's score is a person's total grade as {I_{DIK2}} $\xrightarrow{K_{DIK}}$ {D_{DIK4}}.

AVA_I refers to recovering I_{DIK} from inappropriate operations. For instance, AVA_I of I_{DIK1} is protected with {I_{DIK1}} $\xrightarrow{TN_{I-D}}$ {D_{DIK}}. Assume that target I_{DIK1} is modified, we obtain I_{DIK1} from D_{DIK} = {D_{DIK1}, D_{DIK2}, D_{DIK3}, D_{DIK4}} with K_{DIK} in which the definitions of ascending order, descending order, or disorder is {D_{DIK}} $\xrightarrow{K_{DIK}}$ {I_{DIK1}}.

Algorithm 3 Recover D_{DIK} After Destroying Operations

Input: Inappropriate operations $ACT = \{a_1, a_2, \ldots, a_n\}$;
Output: Recovering $RD_{DIK} = \{rx_1, rx_2 \ldots rx_n\}$ and recovery degree DEG_R;
initial $D_{DIK} = \{dx_1, dx_2 \ldots dx_i \ldots dx_n\}$ $\xrightarrow{ACT}$ $D_{DIK}' = \{dx_1, dx_2 \ldots dx_n\}$;
for each $dx_i \in D_{DIK}'$ do
  if (dxi $\vdash I_{DIK}$) I_{DIK} $\xrightarrow{TN_{I-D}}$ dx_i';
// recovering data from corresponding knowledge
  else if (dxi $\vdash K_{DIK}$) K_{DIK} $\xrightarrow{TN_{K-D}}$ dx_i';
// recovering data from corresponding knowledge
return dx_i';
merge dx_i into RD_{DIK};
compute DEG_R;
end for;

VI. FEASIBILITY BASED SIMULATION

To show the feasibility of our proposed meta-modelling and security protection approach based on meta-modeling towards an interactive cost-driven transformation strategy for TR_{DIK}, we evaluate the design of our proposed solution with numerical simulation. We designed a smart city model in our simulated edge architecture that contains multiple distributed sensors to collect databases, retrieve information bases and reasoning based on knowledge bases to construct DIKW resources for enacting our proposed security protection approaches. The deployment includes position sensors to collect trajectory data, forming spatial-temporal information and enabling implicit tracking functions, video sensors in several areas of the smart city model to collect visual data, and ATM and online shopping records. These sensor nodes collected resources, such as mobile trajectories of people and vehicles, and meal booking lists, and are classified according to an ontological categorization mechanism. Then, we proposed modes and schemas for these resources to be matched in terms of containing the same content but expressed in different types of resources in terms of DIKW, such as the information type resources of moving rhythm of an individual partially contain the age data and gender data of an individual, and some shopping products are good indicators of the identity of a student, which partially indicates the activity shopping habit information. To simplify the simulation,

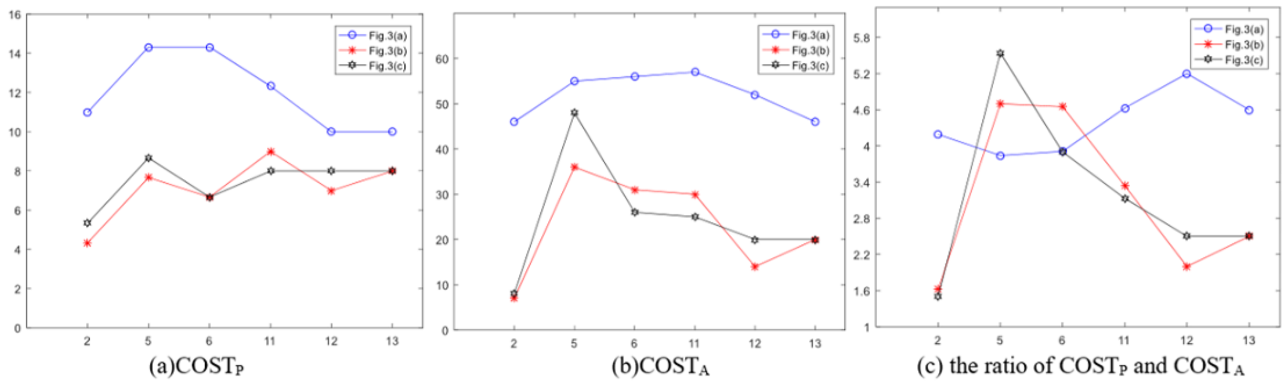


FIGURE 3. Comparison of security context graph and two subgraphs. (a) Comparison of $COST_P$ for the same categories between the security context graph and subgraphs. (b) Comparison of $COST_A$ for the same categories between the security context graph and subgraphs. (c) shows the ratio of $COST_P$ and $COST_A$.

we defined the atomic cost of basic conversions between the smallest unit of various typed resources. Stakeholders are expected to protect resources covering data, information and knowledge that are expressed both explicitly in their original type or implicitly not in their original type. Data type content from four areas (Building 1, Building 2, Building 3 and Building 4) are collected, forming a comprehensive DIKW repository that comprises the background typed DIKW resource graphs of DG_{DIK}, IG_{DIK} and KG_{DIK}. In the background of these graphs, security protection targets are selected from the content or nodes/links of these graphs.

We randomly extracted 20 categories of content resources from the repository and classified them as type D_{DIK} organized in the form of DG_{DIK}. We marked the extent of expectation of these resources in terms of the complexity of evaluation or identified these content from their background content across all of the DIKW graphs. We also set the expected investment up-bound to reach the expected security protection goal of each category of typed content. We expect to protect 20 categories of typed resources as security resources with our cost-driven transformation-based protection mechanism. Transformations are conducted according to the interactively confirmed protection goal, which allows the expected investment of protection to cover the cost of type conversions in terms of computation, network traffic and storage cost in the edge environment in the DG_{DIK} and associated IG_{DIK} and KG_{DIK}. Fig. 3 illustrates the comparisons of $COST_P$ and $COST_A$ during processing. Finally, we further optimize the resource conversion strategy by further contemplating the possible compositions of basic conversions to maximize the benefit of stakeholders.

VII. CONCLUSION

Shifting computationally intensive work of IoT from the cloud to edge computing has prevailed, especially with the increase in the adoption of 5G communication. Among the considerable benefits of this shift, we must also address the challenge of effectively and efficiently processing increasingly diversified resources in terms of data, information, knowledge and even wisdom from various sources, some of which might be from mobile sources. The traditional method or mode of matching various resources one-by-one might be less effective because the possible space of conversion compositions might be too large to be feasibly traditionally solved. We propose considering various resources from a meta-modeling perspective, and then the metamodel of resources can be reduced to data, information, knowledge and wisdom according to the DIKW model. Towards formally working on solutions at this metamodel level, we proposed formalizing the DIKW resources with reference to our proposed semantic expression model of relationship-defined everything of semantics and our proposed reasoning principles of existence computation (EC) at the existence level. In the application background of security content protection, we constructed a basic mechanism for constructing solutions in terms of resource types of data, information and knowledge in our DIKW hierarchy, which consists of specified graphs of data graphs, information graphs and knowledge graphs. Similar to database usage, we propose using resources of DIKW as a database, information-base, knowledge-base and wisdom-base in the DIKW graph forms of the data graph, information graph and knowledge graph. We illustrated the protection of security resources in aspects including integrity, confidentiality and availability with a transformed mechanism, which provides resource accessory management against computation complexity-based attacks. To optimize protection implementation in a business environment, we make trade-offs based on an interactive cost-driven protection strategy that allows trade-offs among protection expectations in terms of meeting expected protection degree but not necessarily surpassing it, and the minimization of the cost of investment by stakeholders and the cost of quality of services. Currently, when users delete and modify their resources, all the transformations of their resources in different layers in DIKW graphs should be deleted and modified accordingly. However, currently, we are still endeavoring to consistently ensure the correctness of deleting and modifying target resources. We are working on further validating modeling and protecting security provisions for a large scale of data and information

REFERENCES

[1] X. Chen, S. Tang, Z. Lu, J. Wu, Y. Duan, S.-C. Huang, and Q. Tang, "iDiSC: A new approach to IoT-data-intensive service components deployment in edge-cloud-hybrid system," *IEEE Access*, vol. 7, pp. 59172–59184, 2019.

[2] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.

[3] Y. Yin, L. Chen, Y. Xu, J. Wan, H. Zhang, and Z. Mai, "QoS prediction for service recommendation with deep feature learning in edge computing environment," in *Mobile Networks and Applications*. New York, NY, USA: Springer, 2019.

[4] Y. Chen, S. Deng, H. Ma, and J. Yin, "Deploying data-intensive applications with multiple services components on Edge," in *Mobile Networks and Applications*. New York, NY, USA: Springer, 2019.

[5] L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, and J. Chen, "A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment," *Future Gener. Comput. Syst.*, vol. 88, pp. 636–643, Nov. 2018.

[6] Z. Wu, Z. Lu, P. C. K. Hung, S.-C. Huang, Y. Tong, and Z. Wang, "QaMeC: A QoS-driven IoVs application optimizing deployment scheme in multimedia edge clouds," *Future Gener. Comput. Syst.*, vol. 92, pp. 17–28, Mar. 2019.

[7] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, to be published.

[8] W. Zhang, Z. Lu, Z. Wu, J. Wu, H. Zou, and S. Huang, "Toy-IoT-Oriented data-driven CDN performance evaluation model with deep learning," *J. Syst. Archit.*, vol. 88, pp. 13–22, Aug. 2018.

[9] Y. Yin, Y. Xu, W. Xu, M. Gao, L. Yu, and Y. Pei, "Collaborative service selection via ensemble learning in mixed mobile network environments," *Entropy*, vol. 19, no. 7, p. 358, Jul. 2017.

[10] Y. Yin, S. Aihua, G. Min, X. Yueshen, and W. Shuoping, "QoS prediction for Web service recommendation with network location-aware neighbor selection," *Int. J. Softw. Eng. Knowl. Eng.*, vol. 26, no. 4, pp. 611–632, 2016.

[11] H. Gao, W. Huang, X. Yang, Y. Duan, and Y. Yin, "Toward service selection for workflow reconfiguration: An interface-based computing solution," *Future Gener. Comput. Syst.*, vol. 8, pp. 298–311, Oct. 2018.

[12] Y. Yin, F. Yu, Y. Xu, L. Yu, and J. Mu, "Network location-aware service recommendation with random walk in Cyber-physical systems," *Sensors*, vol. 17, no. 9, p. 2059, Sep. 2017.

[13] Z. Song, Y. Duan, S. Wan, X. Sun, Q. Zou, H. Gao, and D. Zhu, "Processing optimization of typed resources with synchronized storage and computation adaptation in fog computing," *Wireless Commun. Mobile Comput.*, vol. 2018, May 2018, Art. no. 3794175.

[14] E. Zheleva and L. Getoor, "Preserving the privacy of sensitive relationships in graph data," in *Proc. Int. Workshop Privacy, Secur., Trust KDD*, Berlin, Germany, 2008, pp. 153–171.

[15] Y. Duan, L. Shao, G. Hu, Z. Zhou, Q. Zou, and Z. Lin, "Specifying architecture of knowledge graph with data graph, information graph, knowledge graph and wisdom graph," in *Proc. 15th Int. Conf. Softw. Eng. Res., Manage. Appl. (SERA)*, London, U.K., Jun. 2017, pp. 327–332.

[16] X. Cui, J. Li, J. Li, J. Liu, T. Huang, and H. Chen, "Research on autocorrelation and cross-correlation analyses in vehicular nodes positioning," *Int. J. Distrib. Sensor Netw.*, vol. 54, no. 4, Apr. 2019, Art. no. 1550147719843864.

[17] G. Q. Xu, J. Liu, Y. R. Lu, X. J. Zeng, Y. Zhang, and X. M. Li, "A novel efficient MAKA protocol with desynchronization for anonymous roaming service in global mobility Networks," *J. Netw. Comput. Appl.*, vol. 107, pp. 83–92, Apr. 2018.

[18] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE ACCESS*, vol. 6, pp. 18209–18237, 2018.

[19] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data security and privacy in cloud computing," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 7, Jul. 2014, Art. no. 190903.

[20] Z. Ghahramani, "Probabilistic machine learning and artificial intelligence," *Nature*, vol. 521, no. 7553, pp. 452–459, May 2015.

[21] K. Gai, K.-K. R. Choo, M. Qiu, and L. Zhu, "Privacy-preserving content-oriented wireless communication in Internet-of-Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3059–3067, Aug. 2018.

[22] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.

[23] P. Tarr, H. Ossher, W. Harrison, and S. M. Sutton, "N degrees of separation: Multi-dimensional separation of concerns," in *Proc. Int. Conf. Softw. Eng.*, Los Angeles, CA, USA, May 1999, pp. 107–119.

[24] H. Ossher and P. Tarr, "Using multidimensional separation of concerns to (re) shape evolving software," *Commun. ACM*, vol. 44, no. 10, pp. 43–50, Oct. 2001.

[25] Y. Duan, L. Shao, X. Yang, X. Sun, Z. Zhou, and L. Yu, "Data, information, and knowledge-driven manipulation between strategical planning and technical implementation for wireless sensor network construction," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 11, Nov. 2017, Art. no. 1550147717743700.

[26] Y. Duan, "Existence computation: Revelation on entity vs. relationship for relationship defined everything of semantics," in *Proc. IEEE SNPD*, Toyama, Japan, Jul. 2019, pp. 139–144.

[27] Y. Duan, "Towards a periodic table of conceptualization and formalization on state, style, structure, pattern, framework, architecture, service and so on," in *Proc. IEEE SNPD*, Toyama, Japan, Jul. 2019, pp. 133–138.

[28] L. Qi, W. Dou, W. Wang, G. Li, H. Yu, and S. Wan, "Dynamic mobile crowdsourcing selection for electricity load forecasting," *IEEE Access*, vol. 6, pp. 46926–46937, 2018.

[29] H. Gao, Y. Duan, H. Miao, and Y. Yin, "An approach to data consistency checking for the dynamic replacement of service process," *IEEE Access*, vol. 5, pp. 11700–11711, 2017.

[30] J. Rowley, "The wisdom hierarchy: Representations of the DIKW hierarchy," *J. Inf. Sci.*, vol. 33, no. 2, pp. 163–180, 2007.

[31] Y. Duan, "Applications of relationship defined everything of semantics on existence computation," in *Proc. IEEE SNPD*, Toyama, Japan, Jul. 2019, pp. 184–189.

[32] Z. Wang, J. Zhang, J. Feng, and Z. Chen, "Knowledge graph embedding by translating on hyperplanes," in *Proc. 28th AAAI Conf. Artif. Intell.*, Quebec City, Quebec, Canada, Jun. 2014, pp. 1112–1119.

[33] L. Qi, S. Meng, X. Zhang, R. Wang, X. Xu, Z. Zhou, and W. Dou, "An exception handling approach for privacy-preserving service recommendation failure in a cloud environment," *Sensors*, vol. 18, no. 7, p. 2037, Jun. 2018.

[34] Y. Xu, L. Qi, W. Dou, and J. Yu, "Privacy-preserving and scalable service recommendation based on simhash in a distributed cloud environment," *Complexity*, vol. 2017, Nov. 2017, Art. no. 3437854.

[35] J. Li, Z. Lu, W. Zhang, J. Wu, H. Qiang, B. Li, and P. C. K. Hung, "SERAC3: Smart and economical resource allocation for big data clusters in community clouds," *Future Gener. Comput. Syst.*, vol. 85, pp. 210–221, Aug. 2018.

[36] A. Rashid, A. Moreira, and J. Araújo, "Modularisation and composition of aspectual requirements," in *Proc. 2nd Int. Conf. Aspect-Oriented Softw. Develop. (AOSD)*, Boston, MA, USA, Mar. 2003, pp. 11–20.

[37] Z. Lu, N. Wang, J. Wu, and M. Qiu, "IoTDeM: An IoT big data-oriented mapreduce performance prediction extended model in multiple edge clouds," *J. Parallel Distrib. Comput.*, vol. 118, pp. 316–327, Aug. 2018.

[38] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, "The KDD process for extracting useful knowledge from volumes of data," *Commun. ACM*, vol. 39, no. 11, pp. 27–34, Nov. 1996.

[39] S. Staab, R. Studer, H. P. Schnurr, and Y. Sure, "Knowledge processes and ontologies," *IEEE Intell. Syst.*, vol. 16, no. 1, pp. 26–34, Jan. 2001.

[40] H. Gao, D. Chu, Y. Duan, and Y. Yin, "Probabilistic model checking-based service selection method for business process modeling," *J. Softw. Eng. Knowl. Eng.*, vol. 27, no. 6, pp. 897–923, 2017.

[41] X. Zeng, G. Xu, X. Zheng, Y. Xiang, and W. Zhou, "E-AUA: An efficient anonymous user authentication protocol for mobile IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1506–1519, Apr. 2019. doi: 10.1109/JIOT.2018.2847447.

[42] X.-K. Du, Z.-H. Lu, Q. Duan, J. Wu, and C.-R. Wu, "LTSS: Load-adaptive traffic steering and forwarding for security services in multi-tenant cloud datacenters," *J. Comput. Sci. Technol.*, vol. 32, no. 6, pp. 1265–1278, 2017.

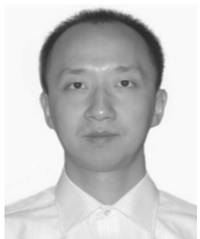
[43] H. Gao, W. Huang, Y. Duan, X. Yang, and Q. Zou, "Research on cost-driven services composition in an uncertain environment," *J. Internet Technol.*, vol. 20, no. 3, pp. 755–769, 2019.

[44] Z. Lu, X. Wang, J. Wu, and P. C. K. Hung, "InSTechAH: Cost-effectively autoscaling smart computing hadoop cluster in private cloud," *J. Syst. Archit.*, vol. 80, pp. 1–16, Oct. 2017.

[45] J. Yang, Z. Lu, N. Wang, J. Wu, and P. C. K. Hung, "Multi-policy-aware MapReduce resource allocation and scheduling for smart computing cluster," *J. Syst. Archit.*, vol. 80, pp. 17–29, Oct. 2017.

[46] K. Benson, R. Dowsley, and H. Shacham, "Do you know where your cloud files are?" in *Proc. 3rd ACM Workshop Cloud Comput. Secur. (CCSW)*, New York, NY, USA, 2011, pp. 73–82.

[47] H. Park and K. Shim, "Approximate algorithms for k-anonymity," in *Proc. ACM SIGMOD Int. Conf. Manage. Data (SIGMOD)*, Beijing, China, 2007, pp. 67–78.
[48] J. Soria-Comas and J. Domingo-Ferrer, "Big data privacy: Challenges to privacy principles and models," *Data Sci. Eng.*, vol. 1, no. 1, pp. 21–28, 2016.
[49] P. G. Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, M. Barcellos, and E. Riviere, "Edge-centric computing: Vision and challenges," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 37–42, 2015.
[50] A. Hundepool, J. Domingo-Ferrer, L. Franconi, S. Giessing, E. S. Nordholt, K. Spicer, and P. P. de Wolf, *Statistical Disclosure Control*. Hoboken, NJ, USA: Wiley, 2012.
[51] S. S. Agaian and O. Caglayan, "Fast encryption method based on new FFT representation for the multimedia data system security," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, Taipei, Taiwan, Oct. 2006, pp. 1519–1524.
[52] W. Eberle and L. Holder, "Discovering structural anomalies in graph-based data," in *Proc. 7th IEEE Int. Conf. Data Mining Workshops (ICDMW)*, Omaha, NE, USA, Oct. 2007, pp. 393–398.
[53] F. D. McSherry, "Privacy integrated queries: An extensible platform for security-preserving data analysis," in *Proc. SIGMOD Int. Conf. Manage. Data*, Providence, RI, USA, 2009, pp. 19–30.
[54] S. Pearson and A. Benameur, "Privacy, Security and trust issues arising from cloud computing," in *Proc. IEEE 2nd Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Nov./Dec. 2010, pp. 693–702.
[55] F. Gong, Y. Ma, W. Gong, X. Li, C. Li, and X. Yuan, "Neo4j graph database realizes efficient storage performance of oilfield ontology," *PLoS ONE*, vol. 13, no. 11, 2018, Art. no. e0207595.
[56] G. Xu, Y. Zhang, A. K. Sangaiah, X. Li, A. Castiglione, and X. Zheng, "CSP-E^2: An abuse-free contract signing protocol with low-storage TTP for energy-efficient electronic transaction ecosystems," *Inf. Sci.*, vol. 476, pp. 505–515, Feb. 2019.
[57] J. Pujara, H. Miao, L. Getoor, and W. Cohen, "Knowledge graph identification," in *Proc. Int. Semantic Web Conf. (ISWC)*, Berlin, Germany, 2013, pp. 542–557.
[58] T. Coffman, S. Greenblatt, and S. Marcus, "Graph-based technologies for intelligence analysis," *Commun. ACM*, vol. 47, no. 3, pp. 45–47, 2004.
[59] G. R. Hjaltason and H. Samet, "Properties of embedding methods for similarity searching in metric spaces," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 5, pp. 530–549, May 2003.
[60] P. Minervini, N. Fanizzi, and C. D'Amato, and F. Esposito, "Scalable learning of entity and predicate embeddings for knowledge graph completion," in *Proc. IEEE 14th Int. Conf. Mach. Learn. Appl. (ICMLA)*, Miami, FL, USA, Dec. 2015, pp. 162–167.
[61] M. Chein and M. L. Mugnier, "Graph-based knowledge representation: Computational foundations of conceptual graphs," *Univ. Aberdeen*, vol. 13, no. 3, pp. 329–347, 2009.
[62] M.-L. Mugnier, "Knowledge representation and reasonings based on graph homomorphism," in *Proc. 8th Int. Conf. Conceptual Struct. (ICCS)*, Berlin, Germany, 2000, pp. 172–192.
[63] J. F. Sowa, *Knowledge Representation: Logical, Philosophical, and Computational Foundations*. Belmont, CA, USA: Brooks/Cole Press, 1994.
[64] M. Chen, D. Ebert, H. Hagen, R. S. Laramee, R. van Liere, K.-L. Ma, W. Ribarsky, G. Scheuermann, and D. Silver, "Data, information, and knowledge in visualization," *IEEE Comput. Graph. Appl.*, vol. 29, no. 1, pp. 12–19, Jan./Feb. 2009.
[65] S. Alonso-Monsalve, F. García-Carballeira, and A. Calderón, "Fog computing through public-resource computing and storage," in *Proc. 2nd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Valencia, Spain, 2017, pp. 81–87.
[66] L. Shao, Y. Duan, L. Cui, Q. Zou, and X. Sun, "A pay as you use resource security provision approach based on data graph, information graph and knowledge graph," in *Proc. Int. Conf. Intell. Data Eng. Automated Learn. (IDEAL)*, Guilin, China, 2017, pp. 444–451.
[67] W. Li, Y. Xia, M. Zhou, X. Sun, and Q. Zhu, "Fluctuation-aware and predictive workflow scheduling in cost-effective infrastructure-as-a-service clouds," *IEEE Access*, vol. 6, pp. 61488–61502, 2018.
[68] J. Guerra, H. Pucha, J. S. Glider, W. Belluomini, and R. Rangaswami, "Cost effective storage using extent based dynamic tiering," in *Proc. 9th USENIX Conf. File Storage Technol. (FAST)*, San Jose, CA, USA, 2011, p. 20.
[69] S. Sardellitti, G. Scutari, and S. Barbarossa, "Joint optimization of radio and computational resources for multicell mobile-edge computing," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 1, no. 2, pp. 89–103, Jun. 2015.
[70] C. Pechsiri and R. Piriyakul, "Explanation knowledge graph construction through causality extraction from texts," *J. Comput. Sci. Technol.*, vol. 25, no. 5, pp. 1055–1070, 2010.
[71] Y. Duan, L. Zhan, X. Zhang, and Y. Zhang, "Formalizing DIKW architecture for modeling security and privacy as typed resources," in *TridentCom* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 270. Cham, Switzerland: Springer, 2018.
[72] Y. Duan, C. Cruz, and C. Nicolle, "Identifying objective true/false from subjective yes/no semantic based on OWA and CWA," *J. Comput.*, vol. 8, no. 7, pp. 1847–1852, 2013.
[73] Y. Duan and C. Cruz, "Formalizing semantic of natural language through conceptualization from existence," *Int. J. Innov., Manage. Technol.*, vol. 2, no. 1, P. 37, 2011.
[74] P. P. S. Chen, "The entity-relationship model—Toward a unified view of data," *ACM Trans. Database Syst.*, vol. 1, no. 1, pp. 9–36, 1976.
[75] I. Kant, *Critique of Pure Reason*. Cambridge, U.K.: Cambridge Univ. Press, 1999.
[76] A. Schopenhauer, *The World as Will and Representation*. London, U.K.: Routledge Press, 1998.



YUCONG DUAN received the Ph.D. degree in software engineering from the Institute of Software, Chinese Academy of Science, China, in 2006. He was a Postdoctoral Fellow with the School of Software, Tsinghua University, China, from 2006 to 2007. He was a Postdoctoral Fellow with the Software Engineering Laboratory, Pohang University of Science and Technology (POSTECH), South Korea, from 2007 to 2008. He was a Lecturer with the Biomedical Engineering Institute, Capital University of Medical Sciences, Beijing, China, from 2008 to 2009. He was a Postdoctoral Fellow with the Le2i, CNRS, University of Bourgogne, France, from 2009 to 2010. He was a Postdoctoral with the DISCO, University of Milano Bicocca, Milano, Italy, from 2011 to 2012. He is currently a Full Professor and a Vice Director with the Computer Science Department, Hainan University. His research interests include service computing, knowledge graphs, and big data. He is also a Senior Member of CCF.

XIAOBING SUN received the bachelor's degree in computer science and technology from the Jiangsu University of Science and Technology, in 2007, and the Ph.D. degree, from the School of Computer Science and Engineering, Southeast University, in 2012. He is currently an Associate Professor with the School of Information Engineering, Yangzhou University. He has authored more than 20 patents and published more than 80 papers in refereed international journals (STVR, IST, JSS, SCIS, and FCS) and conferences (ICSE, ASE, ICSME, SANER, and ICPC). His research interests include software maintenance and evolution, software repository mining, and intelligence analysis. He is a Senior Member of CCF and a member of ACM.

HAOYANG CHE received the Ph.D. degree from the Institute of Software, CAS, in 2006. He is currently a general Manager with the Data Intelligence Center, Auto-Smart Inc. He has authored more than ten books and published more than 20 papers in refereed international journals and international conferences. His research interests include big data, data intelligence, and 3D printing.

CHUNJIE CAO received the Ph.D. degree in cybersecurity from Xidian University, in 2008. He is currently a Vice Dean and a Professor with Hainan University, China. His research interests include big data, cloud computing, cybersecurity, and artificial intelligence. He is also a Senior Member of CCF.

ZHAO LI completed the Ph.D. degree with a Graduate Award from the Computer Science Department, University of Vermont under the Supervision of Prof. X. Wu. He is currently a Senior Staff Scientist with the Alibaba Group, specializing in ecommerce ranking and recommendation systems. He has published over 50 papers in prestigious conferences and journals, including NIPS, AAAI, IJCAI, and KDD. His current research interests include adversarial machine learning, network representation learning, knowledge graphs, multi-agent reinforcement learning, and big data-driven security. He is also a Technical Committee Member of the China Computer Federation on Database. He received a Fellowship from NSF EPSCoR.

XIAOXIAN YANG received the Ph.D. degree in management science and engineering from Shanghai University, Shanghai, China, in 2017. She is currently an Assistant Professor with Shanghai Polytechnic University, China. Her research interests include business process management and formal methods.