IEEE *Access*

Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems

EMAN M. ABOU-NASSAR[1]**, ABDULLAH M. ILIYASU**[2,3,4]**, (Senior Member, IEEE),**
PASSENT M. EL-KAFRAWY[1,5]**, OH-YOUNG SONG**[6]**,**
ALI KASHIF BASHIR[7]**, (Senior Member, IEEE), AND AHMED A. ABD EL-LATIF**[1,5]

[1]Mathematics and Computer Science Department, Menoufia University, Shebin El-Kom 32511, Egypt
[2]Electrical Engineering Department, College of Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[3]School of Computing, Tokyo Institute of Technology, Yokohama 226-8502, Japan
[4]School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China
[5]School of Information Technology and Computer Science, Nile University, Giza 12588, Egypt
[6]Department of Software, Sejong University, Seoul 05006, South Korea
[7]Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, U.K.

Corresponding authors: Oh-young Song (oysong@sejong.edu) and Ahmed A. Abd El-Latif (a.rahiem@gmail.com)

ABSTRACT Today, internet and device ubiquity are paramount in individual, formal and societal considerations. Next generation communication technologies, such as Blockchains (BC), Internet of Things (IoT), cloud computing, etc. offer limitless capabilities for different applications and scenarios including industries, cities, healthcare systems, etc. Sustainable integration of healthcare nodes (i.e. devices, users, providers, etc.) resulting in healthcare IoT (or simply IoHT) provides a platform for efficient service delivery for the benefit of care givers (doctors, nurses, etc.) and patients. Whereas confidentiality, accessibility and reliability of medical data are accorded high premium in IoHT, semantic gaps and lack of appropriate assets or properties remain impediments to reliable information exchange in federated trust management frameworks. Consequently, We propose a Blockchain Decentralised Interoperable Trust framework (DIT) for IoT zones where a smart contract guarantees authentication of budgets and Indirect Trust Inference System (ITIS) reduces semantic gaps and enhances trustworthy factor (TF) estimation via the network nodes and edges. Our DIT IoHT makes use of a private Blockchain ripple chain to establish trustworthy communication by validating nodes based on their inter-operable structure so that controlled communication required to solve fusion and integration issues are facilitated via different zones of the IoHT infrastructure. Further, C♯ implementation using Ethereum and ripple Blockchain are introduced as frameworks to associate and aggregate requests over trusted zones.

INDEX TERMS Trustworthness, blockchain, security, interoperability, sustainable healthcare IoT systems.

I. INTRODUCTION

In internet of Things (IoT) applications, healthcare systems use assests of interconnected devices to create IoT networks devoted to healthcare assessment. It is generally recognised that patients afflicted with chronic illnesses, such as hypertension, respiratory diseases or diabetes, require medical, hospital, and emergency services more than those

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

with regular ailments. Healthcare-based IoT (i.e. IoHT for simplicity) are systems that collect information from different sensing devices using middleware. For efficient handling of such heterogeneity, IoHT requires interoperability and trust issues support through IoT context based on Blockchain technology. This utility is considered a key challenge in achieving integration over IoT-environments [1]–[5]. One approach to provide trustworthy IoT information is through a distributed service (transaction) trusted by the entirety of its members, which ensures that the information

stays immutable. Moreover, having a system that ensures data reliability would permit government institutions to share and safely move data with residents [1], [6], [7].

IoT and its applications are increasingly becoming part of our everyday lives. This is certain to accelerate with the pervassiveness of efforts to integrate the physical world into the virtual world via the Internet. Whereas, IoT will provide a medium to communicate and exchange information safely and easily [8], [9]. IoT platforms represent an ever-growing network of several heterogeneous things or components. Things, of which those that do not essentially meet common standards could be made by various manufacturers. Additionally, devices often operate using a retinue of communication technologies, which do not always seamlessly coalesce IoT devices to the Internet as would a typical computer device. To enhance seamless, uninterrupted interaction and communication between such heterogeneous devices and the real-world, interoperable solutions, semantic web (SW) technologies [8], [10], [11] are needed. The Semantic Web (SW) technology can be utilised in various layers of IoT infrastructure to connect heterogeneous IoT objects. Numerous IoT models using semantic data models and technologies have been suggested [9], [12] to help manage objects and their meta-data, enrich the knowledge representations for the heterogeneous IoT objects and provide guidance for constructing new IoT systems.

In the context of IoT, the importance of semantic knowledge was discussed in [13], including discussions on where anthologies of objects and/or things could offer benefits in terms of standardisation (i.e. interactions through heterogeneous devices and data providers), interoperability (i.e. precise addressing by advances in IoT-specific semantic technologies), or "things" discovery and search (where semantic annotations and metadata are highly relevant) as well as "semantically driven code generation for device interfaces" [9], [12], [14], [15].

Despite success in simultaneous parallel creation of IoT systems-based ontology, a universal coding language or common communication protocol remains elusive. For this reason, interoperability and other issues became more complex. Meanwhile, it has been suggested that these issues can be curtailed or circumvented through semantic annotation of IoT resources [9], [16], [17]. These solutions involve targeted enhancement, aggregation and filtering of data. Furthermore, it helps to enforce a well-founded hierarchy of the linked data sources since the heterogeneously interconnected resources represented by IoT paradigm require a common language to boost the interoperability between the resources as well as offer homogeneous outcomes when multiple resources are queried. Finally, this system must secure and maintain confidentiality between different nodes on the IoT network [10], [18]–[25].

Encouraged by the above contributions and our intuition to prioritise trust in day to day interactions, focus is given to ensuring that IoT systems with improved interoperability can also secure and guarantee confidentiality between

nodes on the IoT infrastructure. Consequently, efforts around buffering decentralised, autonomous and trust capabilities of Blockchains as building blocks of efficient IoT infrastructure is on the increase [11], [18]–[20], [26]. Moreover, as the systems interact, standard and safe interoperability must be maintained by enhancing a bottom-up structure to secure every node added to the network. Blockchain technology provides the framework to realise reliable, secure and efficient IoT infrastructure. [10], [16], [17], [22]–[24], [27].

Based on the foregoing overview on progresses recorded and challenges in IoHT, contributions of our study include:

1) Providing a privacy-aware management framework to preserve sensitive data of patients
2) Enhancing encryption and IoHT access control methods
3) Improving the security and interoperability mechanisms to support privacy preservation while circumventing pervasive tracking and profiling.
4) Ensuring confidentiality and integrity of patients' data via IoT-based Multi-Cloud solutions in cases of data compromise through insider attacks.

To deliver on the enumerated objectives, the remainder of our study is outlined as follows. To establish the foundation for our proposed decentralised, interoperable, trustworthy Blockchain framework for healthcare IoT (DIT IoHT), we present, in Section 2, overviews covering advances in relevant technologies, such as ontology-based IoHT, Blockchain-based IoHT, etc. Following that, in Section 3, we present and discuss our proposed DITrust Blockchain IoHT framework as well as its implementation. In Section 4, we present an analysis of the performance of our proposed framework alongside established as well as recent methods.

II. ONTOLOGY-BASED IoHT

Creation of ontologies for IoT frameworks is a daunting task that requires expertise from different fields as well as data gathering, analysis and unification into an efficient ecosystem. Such ontologies require high level domain semantics that can coalesce with other web resources.

The practical use of semantic procedures and tools requires formulation and availability of explicitly expressed ontologies, represented using a standard ontology language (such as RDF Schema or OWL). Ontologies are responsible for describing and addressing nodes like sensors, objects, actuators, devices, services and providing the essential level and/or layer of abstraction to deal with heterogeneity and interoperability [12], [28]. Additionally, to support higher level operations, ontologies are concerned with data models as well as interpretations and reasoning coming from sensors and other data produced by devices.

Ontologies offer enhancements to the information model and provide semantic augmentation as well as address cited weaknesses of data models. Additionally, they provide semantic expressiveness to the information and support the exchange of information between applications and

between different levels of abstraction, which is considered a significant goal of IoT environments. Further, ontologies enhance interoperability between different objects by providing uniquely harmonious models representing concepts and relationships between them, which together form a description of some domain. Ontologies with integration of information have been reported in [29]–[32].

Meanwhile, many existing ontologies are concerned with data modeling, linked data using a Trible type, semantic annotation, device representation, object discovery, and semantic sensor network (SSN). A few of these ontologies are highlighted in the sequel.

1) LINKED DATA

Necessary, some requirements are needed for efficient IoT frameworks, such as: successful integration mechanisms for IoT data as well as the network's interoperability through different domains. Access to domain knowledge and semantically enriched descriptions of relevant data (on the web) are necesssary requirements for IoT efficiency. One way IoT data is consumed and published is via a Linked Data (LD) model, which is a method for enriching structured data so that it can be interlinked using semantic queries. Furthermore, LD encapsulates all the semantically annotated information by formatting it using semantic web technologies such as Resource Description Framework (RDF) standard [33]. Several studies have focused on describing the physical "things" used in IoT ecosystems. For example, Datta and Bonnet [34] described the "things" in a uniform fashion using Constrained RESTful Environments (CoRE) link format that measures the sensors and commands for actuators using enhanced Sensor Markup Language (SenML). Similarly, So [35] suggested a lightweight framework for describing and managing smart Machine to Machine (M2M) devices. Taking into account the semantics, the contributions in [34] and [35] are considered foundations for introducing lightweight "thing" management frameworks using (JSON) (Java Script Object Notation) [36]. They used JSON for Linking Data (JSON-LD) and Thing Description (TD) for "thing" description to convert from CoRE link format to semantic-based descriptions.

2) SENSORS AND ACTUATORS

Semantic Sensor Network (SSN) is an ontology widely used in describing sensors and related concepts. It is used as a base for extending other ontologies [37], [38]. The SSN ontology was developed by W3C Semantic Sensor Network Incubator Group to serve as a starting point for sensor related ontologies like "INTER-IoT-Interoperability of Heterogeneous Platforms with the Internet of Thing" projects and OpenIoT ontology.

In a closely related effort, Zgheib [39] explored semantic data sources aggregation from patient sensor networks for semantic representations of sensors using a publish/subscribe architecture. Additionally, a software architecture that depends on a message-oriented middleware driven by semantic OWL messages to ensure interoperability between system components was introduced.

3) MULTI-AGENT SYSTEM (MAS)

The heterogeneous sources in multi-agent systems (MAS) can be dynamically represented in the form of specialised agents capable of communicating, processing and gathering received data. Further, MAS is considered more suitable for very large distributed systems. Its agents can form incorporated groups to solve a problem in a cooperative manner [40]. Here, to benefit from the multiple processors inherent in the infrastructure, the problem is divided into smaller parts. These parts can be distributed over the group equally, hence, a candidate solution can be found faster since some of these parts are executed in parallel [40]. Messages can be sent to an agent without knowing if the agent is running on the same machine or on another one within the network. In this regard, Manate et al. [12] analysed and modelled some existing approaches to semantically describe the "Things" or "objects" within an IoT context. To facilitate expansion and enhance utility, their model was constructed as a multi-agent system. Moreover, the agents buoy up scalability since the agent bus can be bridged over multiple hosts. This model exhibited high interoperability, reliability, scalability and availability.

4) SEMANTIC DATA MODELING

Vastly distributed and heterogeneous characteristics concomitant with IoT resources and networks are known to cause problems such as interoperability and object discovery. Therefore, semantic data modelling is used to resolve these problems, by improving operations like filtering, searching and data aggregation. Further, they are credited with enriching the knowledge representations for loT objects and provide a guideline for constructing new loT systems. However, most of these models cannot provide good inference and efficient interoperability. Meanwhile, as adduced earlier, semantic web ontologies have continued to become very important tools for solving the interoperability problems, especially when several systems that use various data representations and languages interact with each other. Furthermore, ontologies enrich the information model, provide semantic augmentation, improve expressiveness to the information and address the cited weaknesses of data models [12], [17]. Therefore, ontologies can also provide a good formalisation language with logical inference ability to support information exchange between different levels of abstraction and between applications that are important goal of IoT systems.

As illustrated in Figure 1, ontology-based models are suitable for complex concepts and relationship expression. Ontologies are responsible for making pledges in form of cognitive relationships, which entails use of a vocabulary in ways consistent to different domains of applications [9], [14], [15]. In their contribution on the topic, Hachem et al. [15], presented core challenges for building applications that will manage and handle IoT resources (scale, deep
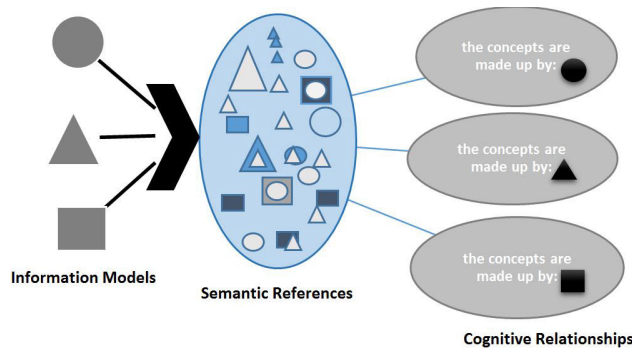
FIGURE 1. Concept of Ontology-based IoHT.

heterogeneity, unknown topology, inaccurate or incomplete data and conflict resolution). To overcome some of these issues, they proposed a new IoT middleware based on specific ontologies. The backbone of their middleware consists of a knowledge base which models all three IoT-layers and contains three ontologies: device ontology (i.e. device description repository through physical layer), domain ontology (which models data about physical concepts and their relations through information layer) and an estimation ontology (which covers the information about diverse estimation models, including "naive Bayesian learning, Kalman filter", equations and services that derive and implement them). Finally, these ontologies are modelled to provide interoperability and flexibility and to describe the ontologies more precisely.

In a closely related effort, in [9], Sejin proposed an IoT directory system (IoT-DS) that includes the semantic description, discovery and integration of IoT things/objects. Operations such as modifying, adding and removing semantic facts, capturing objects and their relationships to construct and reconcile ontology are essential requirements for Semantic Data Platforms (SDP) [14]. Therefore, in that study Semantic IoT Framework was built on SDP to facilitate declarative fact-oriented approach to model where they are executed. Their proposed semantic IoT framework consists of an event manager, as well as data processing and analytic engines that enable clients' assessment of data to make changes when needed.

There are also other ontology studies focused on semantic data modeling such as in [41], and [42]. In [41], the authors are utilized Semantic Information Broker (SIB) for applications on localised computing environments, and therein presented a SIB design for smart spaces based on the M3 architecture (i.e. multi-device, multivendor, multi-domain). This design was touted to support agent interaction in smart spaces by sharing and self-generating information and its semantics. This modular approach was applied for high dependability, extensibility and portability. Similarly, using semantic middleware, in [42], Cassar *et al.* introduced a hybrid semantic service matchmaker for frame IoT works. They integrated probabilistic matchmaking with logical signature matchmaking to overcome problems associated with semantic synonymy.

A. BLOCKCHAIN-BASED IoHT

Blockchain technology provides a paradigm shift in securing ways we share information. The prospect of suffusing Blockchain infrastructure into existing healthcare frameworks is intriguing. This will offer improvements in decentralised storage, distributed ledger, interoperability, authentication, trustworthy, immutability as well as the opportunity to facilitate secure and exceptionally effective interactions between nodes (i.e. patients, healthcare providers, suppliers, etc.) on the healthcare IoT network (i.e. IoHT). Moreover, such nodes could be progressively and efficiently increased and managed. Other benefits of Blockchain suffused IoHT include improvements to system integration, coherence, confidentiality and compliance.

A Blockchain "Distributed ledger", which is defined as a database that keeps up a ceaselessly increasing arrangement of information records, is naturally conveyed implying that the absence of a master PC holding the whole chain. It is scalable with most nodes duplicated and new data readily abutted to extend the chain [19], [20], [26], [43], [44].

Typically, a Blockchain comprises of two components: transactions, which are the events made by the members in the system, and blocks, which record the transactions and ensure their arrangement is unaltered. Further, a Blockchain is decentralised so that no authority can unilaterally endorse transactions or set explicit standards to have transactions accepted. This means that all nodes on the chain must arrive at a consensus before transactions are accepted. Additionally, it must be temper-proof, scalable platform where past records cannot be modified (but, justified cases can be considered subject to additional expenses) [7], [20], [45], [46].

When a new transaction is to be added to the chain, all the participants in the network must validate it. They do this by applying an algorithm that verifies the transaction. However, what is understood as "valid" is defined by the Blockchain system and can differ between systems. Therefore, the power to agree whether the transaction is valid is decided by a majority of the participants.

A set of approved transactions is then bundled into a block that is sent to all the nodes on the network. They, in turn, validate the new block, where each successive block contains a hash, which is a unique fingerprint, of the previous block [20].

B. OVERVIEW OF RELATED LITERATURE

Despite advances in many areas, there is still a difficulty in transferring trustworthy, reliable data through heterogeneous devices and interfaces, which is attributed to semantic gaps and incompatibility. Recently, there has been a lot of potential in deploying IoT in healthcare systems. A review of digital healthcare systems indicates various services, prototypes and a plethora of trust models designed for distributed environments. Some of which are compatible and others are not due to semantic gaps as well as lack of interoperability [16], [18], [47], [48]. To handle heterogeneous platforms and trust domains, Guangyi proposed a UIF (user interoperability framework) with focus on

improving interoperability between IoT devices [16]. Similar efforts are reported in [17], [49], [50] where existing knowledge-based representations are used to annotate metadata and stream sensory data to improve interoperability. In which devices are both syntactically and semantically transformable between their representations of different contexts.

Meanwhile, in utilising RESTful (Representational State Transfer) [51], Blackstock reported integrity-based web services through IoT hubs to aggregate "things" using web protocols. In [52], a variant of Semantic Gateway as Service (SGS) was proposed as a bridge between nodes and IoT services tailored to provide interoperability. This had been achieved by using communication and data standards that relay on SSN ontology as well as translation between them using multi-protocol proxies. In their contribution, in [17], Strassner *et al.* considered enhancing semantic interoperability by providing an extra semantic mapping layer. This layer provides model driver translation against each data source by adding a contextual agent to achieve integration among IoT entities. That framework claims to guarantee that there is no loss or change in the meaning of terms and objects in one device or system when exchanged or used by other devices or systems. Further, in [50], Androcec *et al.* introduced interoperability and semantic layers to enhance integrity between objects over diverse silos.

The heterogeneity of electronic health records (EHRs) in healthcare-IoT systems (i.e. IoHT) comes from medical records collected across various service providers, and complexity in accessing as well as reusing such data makes it a vital challenge for realising efficient IoHT. In ameliorating this, in [53], Curcin *et al.* addressed challenges associated with using a complete common layer called Clinical Data Integration Model (CDIM) for data models based on semantic interoperability mechanisms to achieve data integration between two types of models. This framework would be very useful if it could support trustworthy communication between its members [47], [54].

In similar vein, several other studies have been proposed based on centralised building techniques, which accomplish two aspects of trust (expectancy and belief). However, failed in mitigating vulnerabilities associated with maintaining trust in high risk scenarios. This outcome arises because of weak or ineffective measures ascribed to expected trust [55] models. Semantics of trust based on an ontology trust model creates a clear vision and support making trust judgment in web social networks. Unfortunately, their certainty model is not effective through cyberspaces as IoT, which needs an uncertainty model to be effective. In [56], a new vision of trust was proposed with the objective of reconciling the two perspectives (i.e. interpersonal and organisational) of trust. That study elaborates on the effectiveness of the two types of trust based on diffused qualitative comparative analysis (fsQCA). However, their study although focused on chronic diseases (i.e. diabetes or cancer) and so for patient's autonomy was limited due the seriousness of the situation. Even

so, the study overlooked important measurements needed to establish hospital trust, such as country of origin and word of mouth "trust reviews" such as patient's opinion about the doctor they actually interacted with.

Unlike their approach, our ontology model will consider these factors to achieve high level of trust. A new agent to estimate the expectation of an agent's future performance in a given context based on confidence model was proposed in [54]. The model evaluated both its willingness and capacity by using semantic comparison of the current context and the agent's performance in similar past experiences. Similarly, in [57], Bhattacharya *el al.* argued the need to transfer to a material agency of IoT-enabled smart technology drawing on value and trust in such services design. They enhanced trustworthiness and facilitated adoption between tele-healthcare technologies and future designs of related business models services. Furthermore, they enthused that trustworthiness can be enhanced via patients' feedback and perspective as well as their efforts to identify trustworthy service providers [48]. To improve trust value (TV) estimates based on interaction, experience, and reputation for Ubiquitous Healthcare (UH) environments, fuzzy-probabilistic reasoning was used in [18], [58]. Trust can be further strengthened via received feedback upon completion of commitment. As vital factors by reverting to the trust factors for estimating accurate and more robust trust values, dealing with trust factors through a semantic structure for interoperability and comprehensibility across any platform. Blockchain technology is utilised to enhance protection, trustworthiness and management of privacy preferences set by each user of the system. Therefore, no sensitive data is accessed without their consent.

Meanwhile, in [59], Cha considered a Blockchain framework where users set their privacy preferences for the IoT devices they interact with. Doing so ensures that no sensitive data is accessed without users' consent. The integration of Blockchain gateways was similarly proposed in [29] for a setup tailored for use in IoT scenarios. In another contribution, O'Connor assessed good practices to be considered for obtaining user consent for IoT applications in the healthcare domain [55]. Elsewhere, Dubovitskaya *et al.* proposed a prototype Blockchain-based technology to enhance privacy, security, and availability. Authors developed a framework responsible for managing and sharing Electronic medical records (EMR) for cancer patient care [1]. To reduce cost, fine-grained access control is achieved over EMR data. While efficiency was enhanced via structuring patient records as well as metadata and using semantics of healthcare data. This is important since the capability to robustly and securely construct privacy-preserving predictive models for healthcare data is essential.

In [45], an online machine learning based Blockchain (ModelChain) was constructed for privacy preservation. Therein, every participating node contributes to model parameter estimation without revealing any health information about patients. Furthermore, they designed a proof-of-information algorithm to determine the order of online
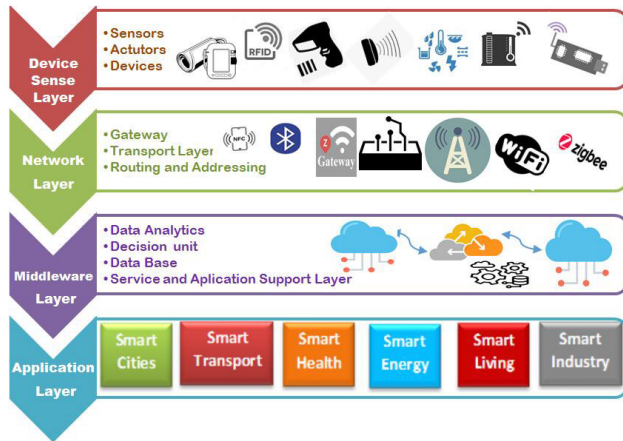
FIGURE 2. Layers of IoT and their components.

FIGURE 3. Security levels for different IoT layers of proposed framework.

learning process and improve interoperability between institutions. In their contribution, [22] implemented zones of trust objects with conformable and reliable bubbles of trusted for followers of each bubble. The framework was touted as one that supplies a solid identification and gadget confirmation with Blockchain enhanced security. Fundamentally, this framework makes secure virtual areas (bubbles) where trust and personality among "things" exist. Finally, in [7], Mamoshina proposed an inclusive road map to study and implement advanced systems to acknowledge prescient investigation of healthcare information and advanced examinations to achieve precision medicine. However, their framework or application is constrained by the need to implement experiments required to assess their quality and shortcomings.

The studies highlighted above, demonstrate the efficient use of Blockchain technology and semantic methodologies to enhance security, trust, authentication and interoperability in medical and healthcare federated frameworks. Using semantic annotation to accomplish data integration, fusion and federation over IoT-silos. They provide foundations on which our DIT Blockchain IoHT framework is built.

III. GENERAL FRAMEWORK OF DITrust CHAIN MODEL
Figure 2 presents the general architecture showing the different layers of our proposed DIT Blockchain IoHT framework. The first layer is dedicated for collecting and processing information as well as making necessary changes to such data. This layer comprises of sensors and actuators required for different functions such as querying location, temperature, blood pressure, weight, motion, vibration, humidity, etc. using standard plug-and-play mechanisms the perception layer can be heterogeneously configured.

The second layer comprises gateways and network paths required to transmit the IoT data. The gateways serve in collecting and securely transporting data from devices, remote users, and applications to execute particular needs. Communication, i.e. network, technologies include Bluetooth, WiFi, ZigBee, RFID, NFC, Wireless Hart etc.

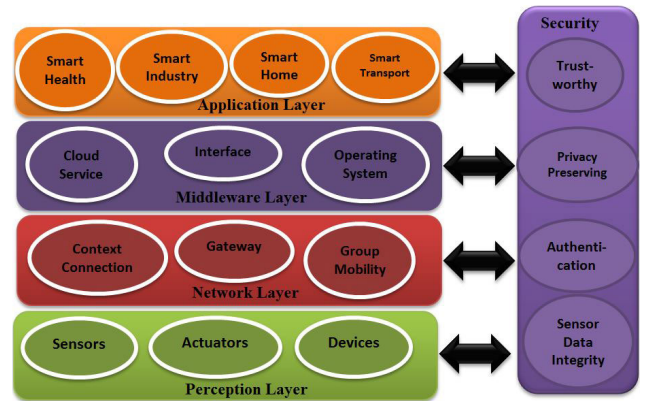The third layer of our framework, also called middleware, consists of interposed sub-layers found between the

technology and application levels. Its capability to hide different technologies is vital for exempting the programmer from issues that are not directly pertinent to her/his focus. Blockchain decision units, data analytics or service as well as application support layers serve as sub-layers of our Healthedge.

Lastly, at the lower end of the architecture we have the application layer where all the system's functionalities are exported to the end users. While not part of the middleware, this layer exploits capabilities of the middleware through its use of standard web service protocols and service composition technologies. This is to realise perfect integration between distributed systems and applications. This process is further illustrated in Figure 2.

Meanwhile, Figure 3 presents the security levels expected based on the enumerated IoT layers of our proposed framework. This comprises of:

1) **Sensor data integrity:** This is accomplished through device sense layer. In our framework, to achieve the integrity between devices, every node has its semantic annotation (semantic-JSON).
2) **Authentication:** This is realised through network and gateway layers. In our model, this is accomplished through public Blockchain based on smart contracts.
3) **Privacy preservation:** This is the security measure required over cloud or middleware layer.
4) **Trustworthiness:** This is the application layer that facilitates trust between members on the IoT network.

A. DITrust BLOCKCHAIN FOR IoHT MODEL
In this section, we present the rudiments of our proposed **D**ecentralised **I**nteroperable **T**rust model (DIT) Blockchain framework for healthcare IoT (IoHT) systems. It is designed to generate reliable cooperative IoT eco-systems (zones) with reliable mutual information integration between its members. In addition, our DIT Blockchain IoHT (DIT IoHT) framework is capable of decentralised, autonomous, transparent storage of interoperable trustworthy transactions. Through it, we present a trusted virtual platform to secure IoT using the architecture of our framework whose outline is presented in
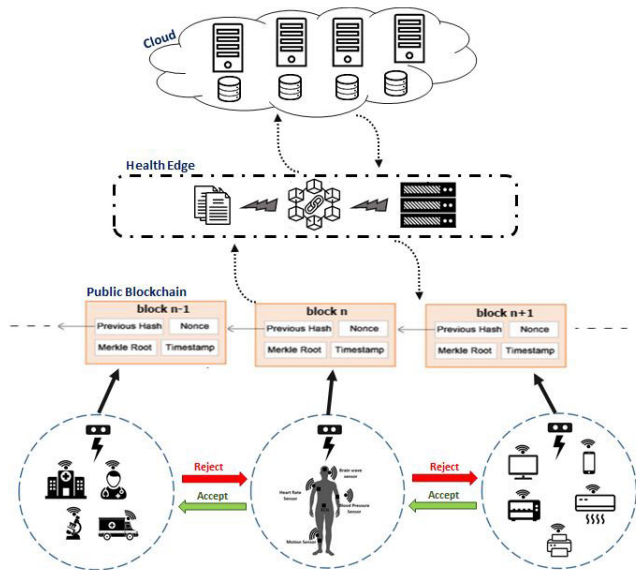
FIGURE 4. Outline of proposed DITrust Blockchain IoHT Model.

Figure 4. In the sequel, we will outline steps of the proposed DIT Blockchain IoHT framework.

1) CREATING TRUSTED VIRTUAL ZONES

By having a public-private key pair, any device can be designated as a primary object. At first, to join a trusted group, a device must be named after the group it seeks to join, i.e. using an identifier (G_ID). Next, to join the trusted zone, every primary object must execute a secure transaction. The first request from any member has to create a trusted zone to have their transaction validated by the Blockchain.

Our proposed model is equipped to handle scalable growth of the IoT infrastructure. Therefore, each object that becomes part of the system is called a member and each member generates a public-private key pair of Elliptic curves (EC). At that point, each member is described by a unique characteristic structure called IDplate comprising of 64 byte lightweight certificate covering Member ID (ObJ_ID), Group ID (G_ID), Public Address (PuB_Addr) and Private tag (Signature).

As presented in Figure 5, information in the IDplate include:

1) **ObJ_ID:** represents identifiers for members in each zone.
2) **G_ID:** refers to the zone that the member is part of.
3) **PuB_Addr:** specifies member's public address, which records the first 20 bytes of the SHA-3 (Keccak) hash of the members' Public key.
4) **Signature:** refers to Elliptic Curve Algorithm (ECA) using a private key of the zone's primary key. The ECA signatures have multiple advantages over traditional algorithms as (such as (*Rivest Shamir Adleman* (RSA) algorithm), like signature times and key sizes. These properties make ECA signatures more compatible to IoT-environments. The Signature is a concatenation of Mem_ID, (G_ID), and PuBAddr based on Keccack hash and signed using the primary private key.
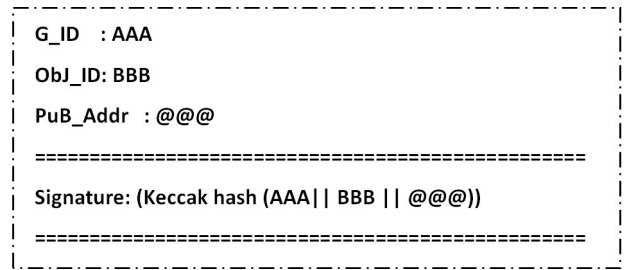

FIGURE 5. Example of IDplate for members in different zones.

Algorithm 1 Definition of Parameters and Functions

1 **Parameters:**
2 *BC*: Blockchain
3 *RC*: Ripplechain
4 *HE*: HealthEdge
5 *ob*: Object
6 *dispatcher*: Object
7 *recipient*: Object
8 const *failed*: State
9 assign *primary*: 0
10 assign *member*: 1
   // check if the object identifier is
   used in the Blockchain or not
11 **Function:** ObIdVerif (Integer *ob_Id*, Blockchain *b*)
   // verify if the group identifier is
   used in the Blockchain or not
12 **Function:** GroupIdVerif (Integer *grp_Id*, Blockchain *b*)
   // verify if the object address is
   used in the Blockchain or not
13 **Function:** AddrVerif (Integer *ob_Addr*, Blockchain *b*)
   // verify if the semantic annotation
   object Sheet (JsonLD) is founded
   in the health-edge or not
14 **Function:** SemSheetVerif (Semantic *ob_Sht*, HealthEdge *e*)
15 **Function:** Fault ()// returns and fault
   message

---

2) EXECUTING THE PROPOSED FRAMEWORK

Execution of the proposed framework involves additional sub-routines as outlined below.

1) The initialisation step, a primary object (which, as mentioned earlier, must have both public and private keys) detects its group using the group identifier (G_ID). Further, every member is distinguished by a signed token that designates its primary object and group.
2) The primary object requests the device to provide a transaction request containing its Ob_ID and G_ID. The public Blockchain is used to construct its unique zone. The Blockchain verifies the veracity of the primary and group IDs and establishes the validity of the transaction to create trusted primary zones. Algorithm 1 elucidates execution of this step of the proposed framework.

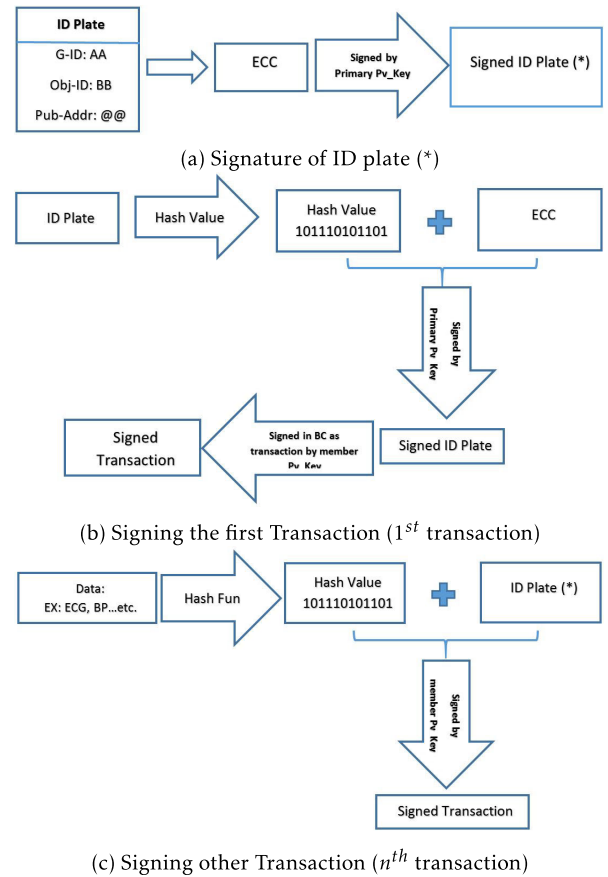**Algorithm 2** Association Rules for Smart Contract Zones

1 **Begin**
2 **if** *(ObIdVerif (ob.id, BC) = true)* **then** return Fault ()
3 **if** (AddrIdVerif *(ob.Addr, BC)= true)* **then** return Fault ()
4 **if** *(ob.type = primary)* **then**
5 **if** *(GroupIdVerif (ob.grpId, BC) = true)* **then** return Fault ()
6 **else if** *(ob.type = member)* **then**
7 **if** (GroupIdVerif *(ob.grpId, BC) = false)* **then** return Fault ()
8 **if** *(BC.*IDplateVerif*(ob.idplate) = failed)* **then** return Fault ()
9 **else** return Fault ()
10 // Association accomplished with success
11 **End**

3) Following the zone creation in step 2, as members send transactions, the Blockchain interface, verifies them using smart contracts. This entails ascertaining the uniqueness of the members' identifiers, i.e. Ob_ID, as well as verifying the legitimacy of the ID plate using the public key of the zone's primary node. This process is outlined in Figure 6. In the unlikely event, that any of the enumerated prerequisites is not satisfied, the incident cannot be linked to any zone nor can the aggregation request be made to another zone. Thus, effectively shutting down any further efforts to execute the request. Algorithm 2 presents this procedure in executable steps. Whenever the main exchange (i.e. association request) is successfully submitted, the verification is seamlessly executed as an exchanged message, Which is illustrated in Figure 6**c**. At the instance, interaction between the object with any member in the trusted zone is facilitated via health edge nodes using Ripple chain restricted communication.

4) Each connected member (with its own primary devices) is tagged to a dedicated zone as a node, i.e. wearable device, smart home, etc.

5) Members in each trusted zone have two types of interactions (association or aggregation) requests. Whereas. the former is restricted to the same trusted zone via public Blockchain. The latter is executed via a different trusted zone that is overseen by a restricted health edge communication portfolios.

It is important to note that the decentralised and immutable nature of Blockchains make it more scalable and interoperable with effective level of reliability. As nothing that is recorded in Blockchain can be modified. Each block in Blockchain (BC) has a cryptographic hash of the previous block so it is resistant to modification of the data. Our proposed model uses two types of Blockchain technologies. First is the Public Blockchain, which is ingrained with the ability to connect every object in the IoT environment. Second,

(a) Signature of ID plate (*)

(b) Signing the first Transaction (1st transaction)

(c) Signing other Transaction (n^{th} transaction)

FIGURE 6. **Signing transaction mechanism where each object's IDplate is signed by private key of the zone's primary key generated using Elliptic Curve Cryptography (ECC).**
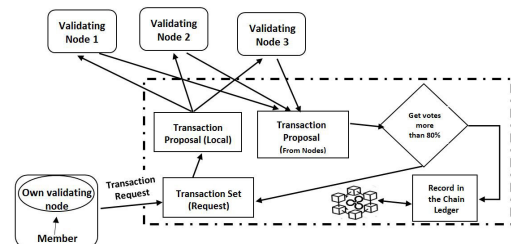
FIGURE 7. **Ripple chain Architecture.**

with Ripple Blockchain, running on a fully permissioned environment, limiting the access to available information, it is easily accomplished through Health-Edge in our framework, thus safeguarding privacy and trust issues over diverse zones. The transaction is not recorded in ripple until it ensures the validation of nodes needed to communicate through JSon-LD algorithm in health-Edge.

Unlike private Blockchain, in Ripple Blockchain, permission is not confined to one organisation or any specified member. It is also unavailable for the purpose of creating transactions. Ripple Blockchain (RBC) provides a mix whose operation is premised on validating leadership of a group (or zone). Where each group has a primary member that detects its group and provides accessibility to every object that has permission.

Meanwhile, all primary nodes in other zones can connect by a controlled communication through a health edge; consisting of a Ripple Blockchain (as outlined earlier in Figure 4) and a smart interoperable structure. In RBC, transactions are initiated by members and broadcasted throughout the network via validated nodes (*primary Devices*). However, the consensus process is accomplished by validated nodes that is comprised of a group of trusted members founded in trusted zones. Members in a trusted zone can vote on the transactions they support. The consensus process in Ripple chain is illustrated in Figure 7. As inferred in that figure, any member of a trusted zone can send a request to its own valid node(s). This authenticated node sends its transaction set as a proposal for validation by a targeted member in its trusted area. Once received, the transaction proposals are sent to validating nodes where the presence of each transaction is in the proposal is vetted. Confirmed transactions are awarded one vote if there is the same transaction in its local transactions request. Next, a set of protocols are used to verify the structure and function of each transaction. When the transaction accumulates more than 80% votes it will be recorded in the distributed record and, henceforth, Ripple is an outright-conclusion consensus protocol.

3) AGGREGATION AND ASSOCIATION RELATIONSHIPS

The relation between members in the same trusted zone are called (association relationships) and the members in different trusted groups (aggregation relationships) are executed by a primary members in every area. Following is an outline of the requirements of the two requests.

a: ASSOCIATION REQUEST

In an association request, each spot (i.e. in the same trusted zone) executes its transaction using *Ethereum* as Blockchain. Ethereum is considered the second-best ledger after Bitcoin and it generates a cooperative IoT system capable of reliable mutual exchange of information between the members, based on smart contracts that simplify the implementation of transactions between a zone's members. This facilitates secure exchange based on Elliptic Curve Cryptography algorithm (ECC), which provides lightweight and robust signature for members in healthcare system zones.

b: AGGREGATION REQUEST

If authenticated by the Blockchain (i.e. in the first stage), each device can communicate with other devices in its zone (group). In other words, the member can communicate with other devices in other trusted zones through restricted connection using health-edge as depicted in Figure 8. The communicating groups are able to communicate with each other via public key elliptic curve cryptography (ECC) as outlined in Algorithm 3.

Further, a member in one trusted zone can send or receive data from other trusted zones using the general public key of the group. Moreover, the sender or receiver in another side
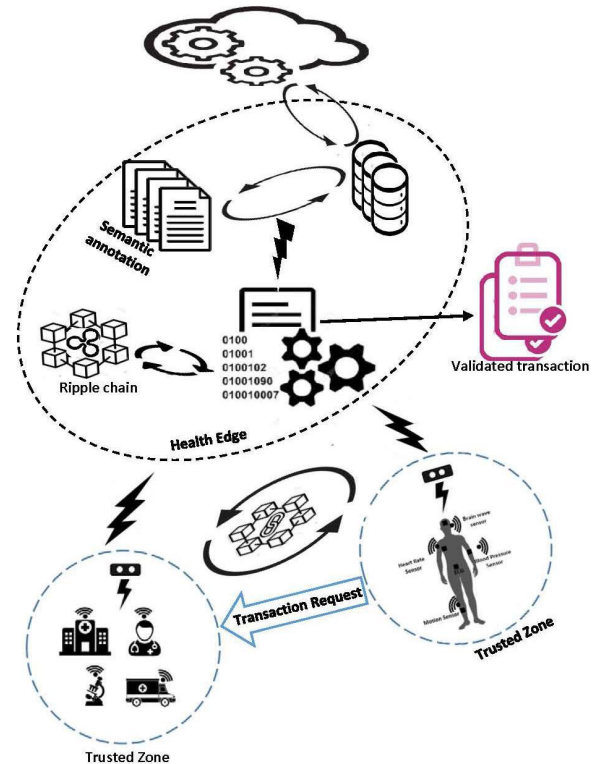
FIGURE 8. Aggregation transaction executed through Health Edge which consists of Ripple chain that is responsible for authenticated validation of the primary nodes, need to create a transaction with another trusted zone based on a published interoperable structure.

Algorithm 3 Aggregation Rules for Smart Communication Zones

---

1 **Begin**
2 **if** (HE.ObIDValid(*ob.id, BC*)= *false*) **then** return Fault ()
3 **if** (HE.GrpIDValid(*ob.grpid, BC*)= *false*) **then** return Fault ()
4 **if** (HE.AddrIDValid(*ob.addr, BC*)= *false*) **then** return Fault ()
5 **if** (HC.SemShtExists(*ob. semsht*)=*failed*) **then** return Fault ()
6 // make matchmaking between sender and
7 // receiver on their semantic sheet style
8 **if** (SemSheetVerif (*dispatcher. semsht, recipient.semsht*) = *false*) **then** return Fault ()
9 // Aggregation accomplished with success
10 **End**

---

can decide to decrypt the content of the secret data using his/her private key.

Based on our proposed architecture, all members in connected trusted zones can trust each other and their communication is inaccessible to non-members and/or untrusted devices. It is secured and guaranteed via public Blockchain, which implements smart contracts instead of private ones that allow any user (member) to join the group and make the system more scalable.

Furthermore, end-to-end security is facilitated via the Blockchain, such that, if some member, M1, sends a message to M2, the message must pass through the Blockchain for vetting. When validated, the message is sent to M2. In contrast, the communication between different trusted zones (such as messages sent to health-edge consummated via Primary nodes in different trusted zones) the matchmaking algorithm accomplishes the communication as outlined in Figures 7 and 8. The algorithm is based on specified interoperable structures, uploaded on health-edge by every trusted zone.

On the Health-edge, requests from the aggregation transactions pass through a verification set to validate its safety upon which permission for communication with other trusted zones is granted.

Meanwhile, the Health-edge layer hosts the semantic annotation file for each node in its zone as a lightweight data interchange format based on JSON-LD syntax. The messages are carried over communication protocols, and interoperability is achieved because this layer supports readability of symbols and syntax.

The implementation steps and validation of the aggregation request that herald the registration through Ripple chain (RBC) technology as enumerated in the sequel.

1) The aggregation request takes place between two nodes over different edges. The Sender node sends its request to the health-Edge via its primary node. This request is routed through several stages for authentication, following which it is implemented under controlled communication and stored as a transaction in RBC to guarantee privacy and reliability between zones. This process can be further elucidated using the following four steps.

   a) The legitimacy of the transaction is verified to ensure that the primary nodes are valid and authenticated by the public Blockchain (i.e. in preceding layer).
   b) The primary node in the receiver zone sends the approved message to the Receiver.
   c) Using controlled communication rules constructed by Semantic JSON syntax, the edge layer provides a common data interchange format across different zones. For example, *Blood Pressure* Sensor (BPS) in semantic file of one zone can send integer data to a *Doctor* or an *Ambulance* in another zone.
   d) Sender node's semantic file type is checked for concordance with that of the Receiver, following which the edge sends data to all matched nodes in the receiver zone.

2) Once recorded on the ripple chain, the transactions are confirmed within seconds, accruing little cost in the process.

3) The exchanged messages are transmitted between members through two requests as presented earlier (i.e. association and aggregation) regulated using two layers

(public BC and Health-Edge) over IoT middleware layer. Inferred in Figure 2. Here, public BC is responsible for validating the associated requests between members in the same zone; otherwise, Health-Edge is responsible for ensuring the trustworthy communication between members in diverse zones. Moreover, privacy over their valid transactions is acheived through Ripple chain, which guarantees compatibility between communicated nodes in different zones as outlined in Algorithm 4.

Algorithm 4 Exchange Messages' Communication Rules Over Different Zones

---

1 **Begin**
2 // in case of association requests
3 **if** (ObIdVerif (dispatcher.id, BC) = false   or ObjIdverif (recipient.id, BC) = false) **then** return Fault ( )
4 **if** (dispatcher.grpId != recipient.grpId) **then** return Fault ( )
5 **if** (BC.SignVerif (dispatcher.msg) = failed) **then** return Fault ( )
6 // in case of Aggregation requests
7 **if** (HE.ObIDValid(dispatcherj.id, BC)= false
8 **or** HE.ObIDValid(recipient.id, BC = false)**then** return Fault ()
9 **if** (dispatcher.semshttype != recipient.semshttype) **then** return Fault ( )
10 **if** (RC. SignVerif (dispatcher.msg) = failed) then return Fault ( )
11 // Secure information trade got done with success
12 **End**

IV. IMPLEMENTATION OF PROPOSED FRAMEWORK

To guarantee the resilience and supportability presented in Figure 3 for IoT-context where layers of the network must satisfy various security and interoperability prerequisites. In this section, we outline the main security and interoperability objectives and requirements for our proposed framework. As well as the criteria required to asses the appropriateness of authentication plans to make IoT use cases more secure.

A. EVALUATION OF SECURITY ISSUES

Table 1 presents a comparison of the evaluation criteria for our proposed model alongside similar methods whose further details are provided in the sequel.

1) SCALABILITY

Scalability considers the capacity to guarantee that the framework size has no effect on its performance. In our study, a peer to peer network supports two types of communication - associated and aggregated requests. Whereas a public Blockchain is used in the former to cover association requests, the latter uses a health-edge to facilitate controlled communication on aggregation request between members over different zones

TABLE 1. Checklist for IoHT evaluation criteria relative to cited literature.

Features	[22]	[60]	[61]	Proposed framework
Scalability	–	√	√	√
Interoperability	–	√	–	√
Availability	√	–	√	√
Mutual Authentication	√	–	–	√
Trustworthy	√	–	–	√
Data integrity	√	√	√	√
Authentication mechanism	√	–	√	√
Confidentiality and Privacy	–	–	√	√

using semantic Json-LD. Unlike the controlled communication issue in [22], our proposed approach is scalable.

2) MUTUAL AUTHENTICATION
Our authentication mechanism implies use of a validation technique similar to those used by Hammi *et al.* [22] and Rahman *et al.* [61]. However, our approach includes an authentication mechanism that uses a public Blockchain. Consequently, our mutual authentication implies the need for end to end authentication i.e. parties must validate credentials of each other. This safeguards the framework from spoofing. Unlike our tamper-proof framework, the absence of the security layer in [61] implies that any device can consummate a transaction with another without ascertaining their identity or confirming any mutual authentication between devices. In the proposed DIT IoHT framework, each gadget has an ID plate signed by its primary key that associates it to a trusted zone and ensures the legitimacy of objects. All transactions are signed using private keys generated using ECC algorithm, which further safeguards the integrity of exchanged messages between nodes.

3) TRUSTWORTHINESS
Like [22], the reliability between members is assessed using hashing and a signed exchanged messages. The signatures generated using the elliptic curve signature algorithm ensure the trustworthiness and seamless of data integration between members. In contrast, in [61] entities do not trust each other. Additionally, in their framework any device can share its transaction over the Blockchain without confirming the reliability and validity of the resource. The study does not elucidate how the identity or trust issues between members is guaranteed prior to execution of trusted transactions between them.

4) PRIVACY
As outlined earlier in this section, the privacy or confidentiality of our system is realised using Health edge through Ripple chain based on validated nodes. Which are associated with the transactions taking place between different zones as dictated by controlled communication. If each member's sheet (need to communicate) are matched through JSon-LD computation and transaction, then the members are validated

through the Health-edge, then the transaction is recorded in Ripple chain on Health-edge, no one can access it except the validated nodes associated with it.

5) DATA INTEGRITY
The methods listed in Table 1 make use of different approaches to safeguard data integrity. In [61], Rahman *et al.* accomplished that via Blockchain and cognitive computing to build a secure and intelligent system. Similarly, Hammi *et al.* in [60] introduced a semantic interoperability model over heterogeneous IoT devices in healthcare environment. Like [22], in our model, data integrity is secured through exchange of controlled messages (i.e. signed transactions and communication) in and out of a members' trusted zones. As outlined earlier in Section 3, our model guarantees that no exchanged messages can be modified or changed over its entire life cycle from one member to another. Moreover, our model has the added safety net that only authorised members can modify data on the framework.

Finally, based on the enumerated security features, we surmise that our proposed DIT Blockchain IoHT framework is resilient and robust to attempts aimed at violating integrity of the data stored, shared or processed on the framework.

B. EVALUATION OF INTEROPERABILITY ISSUES
1) SEMANTIC INTEROPERABILITY
Semantic interoperability presupposes that data exchanged between nodes is understood by the different resources on the framework. Like [60], our proposed model provides semantic descriptions required by each member in its zone and utilises JSON-LD semantic matchmaker to facilitate inter-zonal semantic interactions, i.e. across different zones on the framework. Furthermore, to accomplish controlled communication between members in different zones, data is validated for each entity before attempting to communicate with other nodes.

2) AVAILABILITY
It is important, and oftentimes crucial, that a service is available whenever needed. In this context, valued clients must have unhindered access to nodes and services whenever required. Along these lines, an efficient framework should be flexible enough to withstand denial of service (DoS) attacks. Particularly at nodes that provide authentication related services. Our proposed DIT Blockchain IoHT framework accomplishes this via decentralised construction of its Blockchain, which shields it from DoS attacks. The ability to copy and distribute services over various network nodes ensures, that regardless of an intruder or assailant's attempt to block a node, it cannot impede service availability since it permeates the entire network. This increases the resource demands needed to violate the integrity of the model.
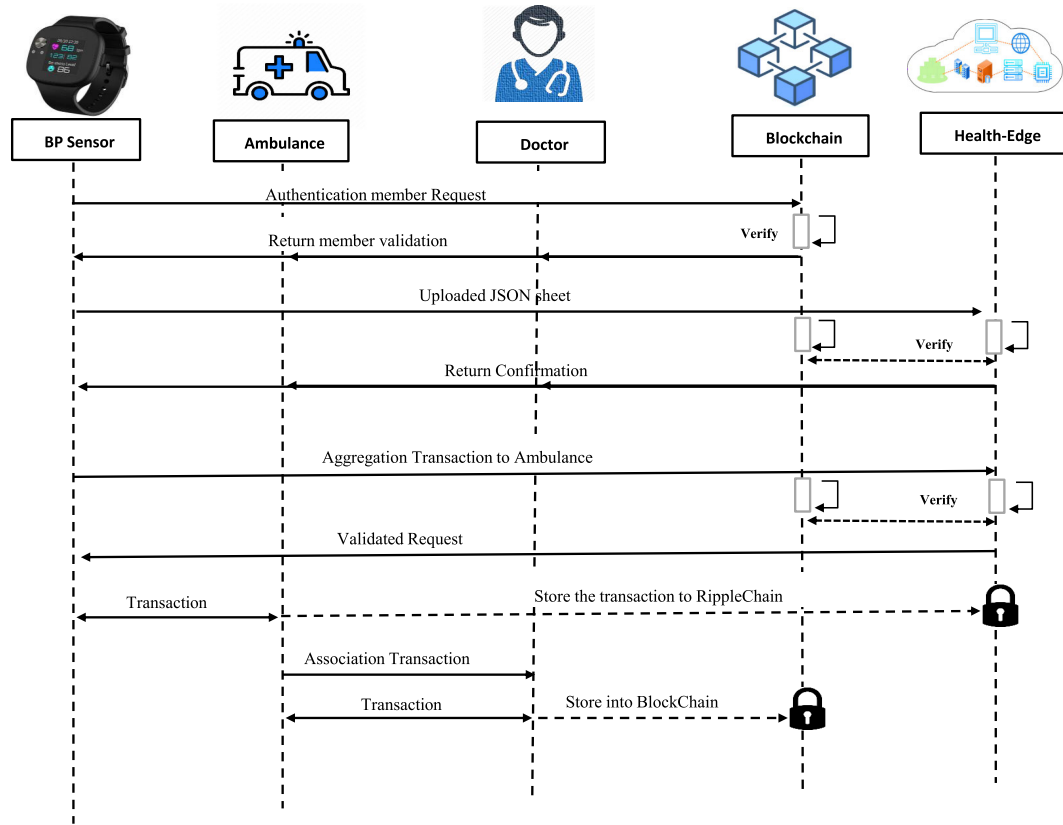
FIGURE 9. Illustration of scenario between Patient, Ambulance and Doctor on DIT Blockchain IoHT framework.

V. CASE STUDY

We conclude discussions on validating our proposed model by considering a case study of the outstanding properties of our framework as enumerated earlier in this section. We consider a scenario comprising of an Ambulance, a Doctor and Blood Pressure Sensor (BPS) as nodes on our IoHT framework. Our objective is to demonstrate the two types of communication (i.e. association and aggregation) requests, that were discussed earlier. The few steps required include:

1) All members are authenticated through a public Blockchain, i.e. Ethereum as used in this study, following which any node can communicate with another node in the same trusted zone, i.e. doctor and ambulance node. The transaction between them called association request and is recorded in Public BC.

2) After authentication phase, each node (i.e. ambulance, doctor and BPS) has the ability to upload its semantic annotation sheet to the Health-edge network.

3) Health-edge layer hosts the semantic annotation file for each node in its zone. Semantic sheets are a lightweight data interchange format based on JSON-LD syntax.

4) In case of aggregation transaction (i.e. doctor and BPs), their sheets are matched with the secure controlled communication rules using JSON Algorithm which ensures validation of each primary node related with the aggregation transaction upon public BC in preceding layer.

5) Finally, after fulfilled matchmaking, the nodes accomplish their transaction and store in Ripple chain, thus making it possible to modify or access the data for nodes related to this transaction, which guarantees date privacy for patients.

1) **Association case** We consider the Ambulance, Doctor or Hospital as example to accomplish association request. The Ambulance service is call Emergency medical service (EMS) provided through medically equipped vehicles that transports patients to treatment facilities, such as Hospitals in IoHT environment. In some instances, out-of-hospital medical care is provided to the patient by referring them to specialists (i.e. Doctors). In our DIT framework, in emergency or special patient cases, EMS communicates with hospitals (via notification messages), for example, to reserve operation theatres. Otherwise, EMS communicates with Specialist by sending patients' case report to prescribe a suitable treatment.

2) **Aggregation case** We consider the Blood Pressure (BP) sensor, Ambulance or Doctor as example to accomplish two types of aggregation requests.
Blood pressure sensor (BPS) used as wearable device can be on patient body. Blood pressure (BP) is the ratio of the systolic to the diastolic pressure expressed in millimetres of mercury, i.e. mmHg. To expatiate,
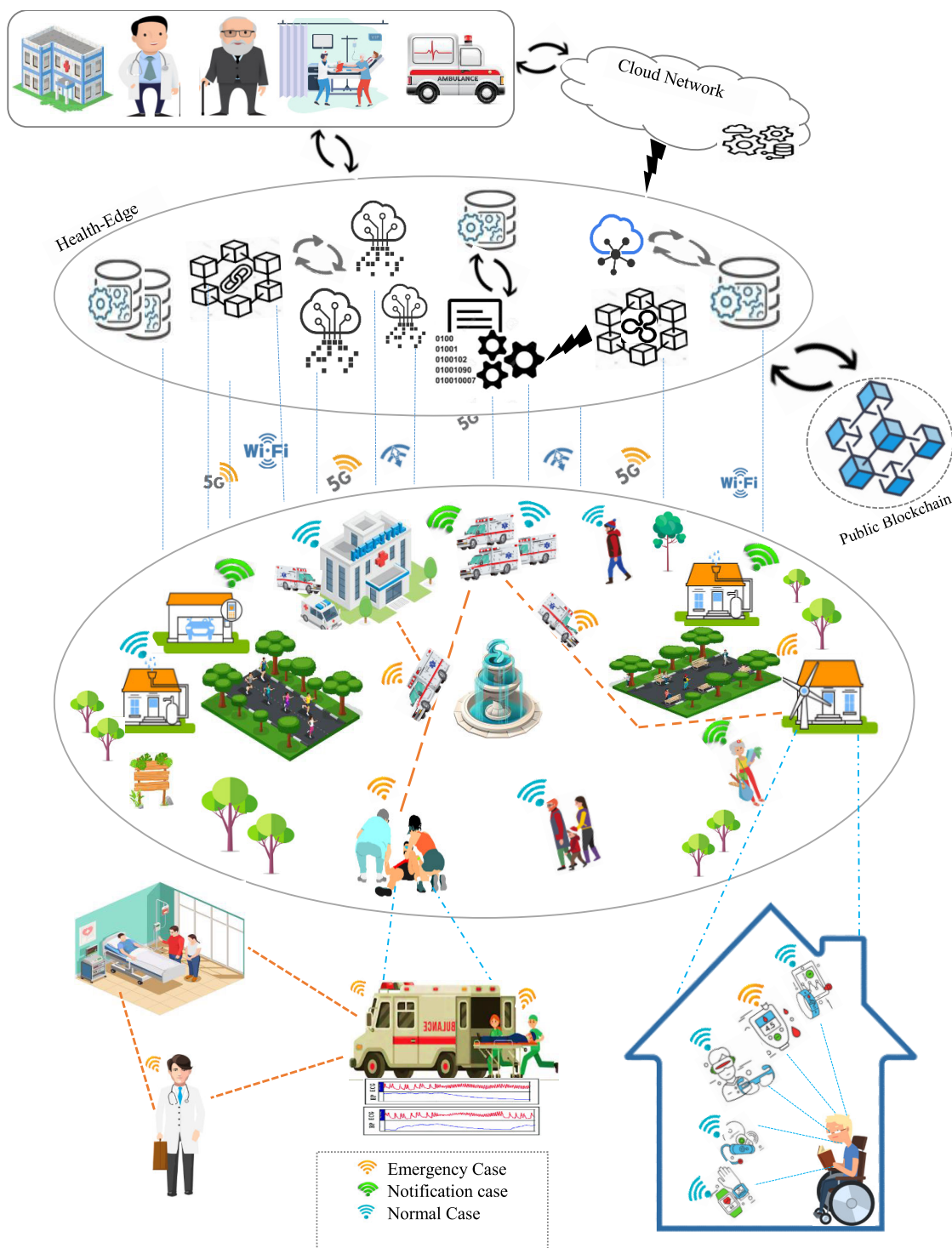
FIGURE 10. Complete scenario illustrating execution of the proposed framework on an IoT-based smart city.

a blood pressure of 140 over 90 or 140/90 mmHg indicates a systolic pressure of 140 mmHg against the diastolic pressure of 90 mmHg. A blood pressure sensor (BPS) is a device capable of automatic detection (i.e. measurement) of blood pressure, usually within fixed intervals per day. Often, BPS are cuff-like devices worn on the wrist and on IoHT networks BPS

communicates its readings to other nodes on the framework, such as an Ambulance or a Doctor. The decision regarding which node this measurement is sent to depends on predetermined thresholds related to the BPS reading, such as severity of ailment, past patient history, etc. For example, depending on a combination of factors, a notification may be sent to the Hospital to

reserve an operation theatre in the same trusted zone or to book an appointment with the Doctor who then decides on a prescription or treatment plan. Either or both scenarios might necessitate correspondence with primary devices on other trusted zones.

The Ambulance description has two potential states:

1) Send a message (Association request) to the Hospital in case of need to open the operation theatre in the same trusted zone or to the Doctor to prescribe appropriate treatment for the patient.

2) Receive the information from patient node (like BPS) in another trusted zone in case of abnormal or special reading mentioned above in case of Aggregation request

Figure 9 illustrates the scenario between Patient, Ambulance and Doctor as explained in our example.

VI. CONCLUDING REMARKS

Blockchain technology provides a veritable platform to secure and enhance efficiency of healthcare-based internet of things (i.e. IoHT) frameworks. Our study proposes a decentralised, interoperable trust model that suffuses Blockchains into healthcare IoHT. Our DIT Blockchain IoHT framework is a resilient ecosystem that supports semantic annotations for health edge layers in IoHT. Cryptographic algorithms are used to authenticate, validate, and secure different stages of data inclusion, exchange, etc. The proposed model outperforms other similar approaches in terms of scalability, interoperability, availability, mutual authentication, trustworthy, data integrity, authentication mechanism, and confidentiality and privacy. As future work, we hope to enhance our framework through the use of artificial intelligence (AI) and deep learning technologies. Specifically, these technologies will be deployed in training stages for the identification of patterns that suggest specific symptoms using information acquired from wearable sensors. Furthermore, we will explore the use of AI as well as machine and deep learning technologies to combine outcomes from different nodes, sensors, etc., such as the BPS and ECGs, to enhance accuracy of disease diagnosis, treatment and management.

ACKNOWLEDGMENT

REFERENCES

[1] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *Proc. AMIA Annu. Symp. Process.*, 2017, p. 650.

[2] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 118–131, Mar. 2020.

[3] A. A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things," *Opt. Laser Technol.*, vol. 124, Apr. 2020, Art. no. 105942.

[4] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud Internet of Things," *IEEE access*, vol. 6, pp. 10332–10340, 2018.

[5] P. K. Khatua, V. K. Ramachandaramurthy, P. Kasinathan, J. Y. Yong, J. Pasupuleti, and A. Rajagopalan, "Application and assessment of Internet of Things toward the sustainability of energy systems: Challenges and issues," *Sustain. Cities Soc.*, vol. 53, Feb. 2020, Art. no. 101957.

[6] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017.

[7] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, and A. Zhebrak, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, p. 5665, 2018.

[8] D. Singh, G. Tripathi, and A. J. Jara, "A survey of Internet-of-things: Future vision, architecture, challenges and services," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 287–292.

[9] S. Chun, S. Seo, B. Oh, and K.-H. Lee, "Semantic description, discovery and integration for the Internet of Things," in *Proc. IEEE 9th Int. Conf. Semantic Comput. (ICSC)*, Feb. 2015, pp. 272–275.

[10] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of Things in healthcare: Interoperatibility and security issues," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 6121–6125.

[11] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[12] B. Manate, V. I. Munteanu, and T. F. Fortis, "Towards a smarter Internet of Things: Semantic visions," in *Proc. 8th Int. Conf. Complex, Intell. Softw. Intensive Syst.*, Jul. 2014, pp. 582–587.

[13] P. Friess, *Internet Things-Global Technological Societal Trends From Smart Environments Spaces to Green ICT*. Gistrup, Denmark: River Publishers, 2011.

[14] A. Palavalli, D. Karri, and S. Pasupuleti, "Semantic Internet of Things," in *Proc. IEEE 10th Int. Conf. Semantic Comput. (ICSC)*, Feb. 2016, pp. 91–95.

[15] S. Hachem, T. Teixeira, and V. Issarny, "Ontologies for the Internet of Things," in *Proc. 8th Middleware Doctoral Symp. (MDS)*, 2011, pp. 1–6.

[16] G. Xiao, J. Guo, L. Da Xu, and Z. Gong, "User interoperability with heterogeneous IoT devices through transformation," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1486–1496, May 2014.

[17] J. Strassner and W. W. Diab, "A semantic interoperability architecture for Internet of Things data sharing and computing," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 609–614.

[18] G. Athanasiou, G. C. Anastassopoulos, E. Tiritidou, and D. Lymberopoulos, "A trust model for ubiquitous healthcare environment on the basis of adaptable fuzzy-probabilistic inference system," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1288–1298, Jul. 2018.

[19] M. Banerjee, J. Lee, and K. K. R. Choo. (2017). *A Blockchain Future to Internet of Things Security: A Position Paper, Digital Communications and Networks.*[Online]. Available: http://www.sciencedirect.com/science/article/piiS

[20] N. Abdullah, A. Hakansson, and E. Moradian, "Blockchain based approach to enhance big data authentication in distributed environment," in *Proc. 9th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2017, pp. 887–892.

[21] J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez, "TACIoT: Multidimensional trust-aware access control system for the Internet of Things," *Soft Comput.*, vol. 20, no. 5, pp. 1763–1779, May 2016.

[22] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018.

[23] P. B. Nichol and J. Brandt, "Co-creation of trust for healthcare: The cryptocitizen framework for interoperability with blockchain," 2016. Accessed: Jun. 1, 2020, doi: 10.13140/RG.2.1545.4963.

[24] T. K. Dasaklis, F. Casino, and C. Patsakis, "Blockchain meets smart health: Towards next generation healthcare services," in *Proc. 9th Int. Conf. Inf., Intell., Syst. Appl. (IISA)*, Jul. 2018, pp. 1–8.

[25] J. Chen, J. Wu, H. Liang, S. Mumtaz, J. Li, K. Konstantin, A. K. Bashir, and R. Nawaz, "Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation," *IEEE Trans. Ind. Appl.*, early access, Dec. 13, 2019, doi: 10.1109/TIA.2019.2959550.

[26] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. E-Health Netw., Appl. Services (Healthcom)*, Sep. 2016, pp. 1–3.

[27] F. Alam Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid, "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development," *Sustain. Cities Soc.*, vol. 55, Apr. 2020, Art. no. 102018.

[28] B. Gateau, Y. Naudet, and J. Rykowski, "Ontology-based smart IoT engine for personal comfort management," in *Proc. 11th Int. Workshop Semantic Social Media Adaptation Personalization (SMAP)*, Oct. 2016, pp. 35–40.

[29] M. Serrano, P. Barnaghi, F. Carrez, P. Cousin, O. Vermesan, and P. Friess, "Internet of Things iot semantic interoperability: Research challenges, best practices, recommendations and next steps," IERC: Eur. Res. Cluster Internet Things, Berlin, Germany, Tech. Rep. IERC-AC4, 2005.

[30] M. Ganzha, M. Paprzycki, W. Pawáowski, P. Szmeja, and K. Wasielewska, "Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective," *J. Netw. Comput. Appl.*, vol. 81, pp. 111–124, Mar. 2017.

[31] E. Mezghani, E. Exposito, and K. Drira, "A model-driven methodology for the design of autonomic and cognitive IoT-based systems: Application to healthcare," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 1, no. 3, pp. 224–234, Jun. 2017.

[32] C. Yang, T.-C. Chou, and Y.-H. Chen, "Bridging digital boundary in healthcare systems—An interoperability enactment perspective," *Comput. Standards Interface*, vol. 62, pp. 43–52, Feb. 2019.

[33] M. Serrano, H. N. M. Quoc, D. Le Phuoc, M. Hauswirth, J. Soldatos, N. Kefalakis, P. P. Jayaraman, and A. Zaslavsky, "Defining the stack for service delivery models and interoperability in the Internet of Things: A practical case with OpenIoT-VDK," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 4, pp. 676–689, Apr. 2015.

[34] S. K. Datta and C. Bonnet, "Smart M2M gateway based architecture for M2M device and endpoint management," in *Proc. IEEE Int. Conf. Internet Things(iThings)*, Sep. 2014, pp. 61–68.

[35] S. K. Datta and C. Bonnet, "A lightweight framework for efficient M2M device management in oneM2M architecture," in *Proc. Int. Conf. Recent Adv. Internet Things (RIoT)*, Apr. 2015, pp. 1–6.

[36] S. K. Datta and C. Bonnet, "Describing things in the Internet of Things: From CoRE link format to semantic based descriptions," in *Proc. IEEE Int. Conf. Consum. Electronics-Taiwan (ICCE-TW)*, May 2016, pp. 1–2.

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

[38] P. Anantharam, P. Barnaghi, and A. Sheth, "Data processing and semantics for advanced Internet of Things (IoT) applications: Modeling, annotation, integration, and perception," in *Proc. 3rd Int. Conf. Web Intell., Mining Semantics*, 2013, pp. 1–5.

[39] R. Zgheib, E. Conchon, and R. Bastide, "Engineering IoT healthcare applications: Towards a semantic data driven sustainable architecture," in *eHealth 360°* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 181, K. Giokas, L. Bokor, and F. Hopfgartner, Eds. Cham, Switzerland: Springer, 2017.

[40] C. Savaglio, M. Ganzha, M. Paprzycki, C. Bǎdicǎ, M. Ivanoviá, and G. Fortino, "Agent-based Internet of Things: State-of-the-art and research challenges," *Future Gener. Comput. Syst.*, vol. 102, pp. 1038–1053, Jan. 2020.

[41] I. V. Galov, A. A. Lomov, and D. G. Korzun, "Design of semantic information broker for localized computing environments in the Internet of Things," in *Proc. 17th Conf. Open Innov. Assoc. (FRUCT)*, Apr. 2015, pp. 36–43.

[42] G. Cassar, P. Barnaghi, W. Wang, and K. Moessner, "A hybrid semantic matchmaker for IoT services," in *Proc. IEEE Int. Conf. Green Comput. Commun.*, Nov. 2012, pp. 210–216.

[43] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[44] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.

[45] T.-T. Kuo and L. Ohno-Machado, "ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," 2018, *arXiv:1802.01746*. [Online]. Available: http://arxiv.org/abs/1802.01746

[46] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, Oct. 2019, Art. no. 101660.

[47] T. Le, G. Salles-Loustau, P. Xie, Z. Lin, L. Najafizadeh, M. Javanmard, and S. Zonouz, "Trusted sensor signal protection for confidential point-of-care medical diagnostic," *IEEE Sensors J.*, vol. 17, no. 18, pp. 5807–5816, Sep. 2017.

[48] G. Athanasiou, M.-A. Fengou, A. Beis, and D. Lymberopoulos, "A trust assessment mechanism for ubiquitous healthcare environment employing cloud theory," in *Proc. 37th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Aug. 2015, pp. 1405–1408.

[49] A. Gyrard, M. Serrano, and G. A. Atemezing, "Semantic Web methodologies, best practices and ontology engineering applied to Internet of Things," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 412–417.

[50] D. Androcec and N. Vrcek, "Thing as a service interoperability: Review and framework proposal," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, pp. 309–316.

[51] M. Blackstock and R. Lea, "IoT interoperability: A hub-based approach," in *Proc. Int. Conf. Internet Things (IOT)*, Oct. 2014, pp. 79–84.

[52] P. Desai, A. Sheth, and P. Anantharam, "Semantic gateway as a service architecture for IoT interoperability," in *Proc. IEEE Int. Conf. Mobile Services*, Jun. 2015, pp. 313–319.

[53] J. F. Ethier *et al.*, "Clinical data integration model. Core interoperability ontology for research using primary care data," *Methods Inf. Med.*, vol. 54, no. 1, pp. 16–23, 2015, doi: 10.3414/ME13-02-0024.

[54] N. Osman, C. Sierra, F. Mcneill, J. Pane, and J. Debenham, "Trust and matching algorithms for selecting suitable agents," *ACM Trans. Intell. Syst. Technol.*, vol. 5, no. 1, pp. 1–39, Dec. 2013.

[55] J. Huang and M. S. Fox, "An ontology of trust: Formal semantics and transitivity," in *Proc. 8th Int. Conf. Electron. Commerce*, 2006, pp. 259–270.

[56] S. Zheng, S. F. Hui, and Z. Yang, "Hospital trust or doctor trust? A fuzzy analysis of trust in the health care setting," *J. Bus. Res.*, vol. 78, pp. 217–225, Sep. 2017.

[57] S. Bhattacharya, D. Wainwright, and J. Whalley, "Internet of Things (IoT) enabled assistive care services: Designing for value and trust," *Procedia Comput. Sci.*, vol. 113, pp. 659–664, 2017.

[58] G. Athanasiou and D. Lymberopoulos, "A comprehensive reputation mechanism for ubiquitous healthcare environment exploiting cloud model," in *Proc. 38th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Aug. 2016, pp. 5981–5984.

[59] S.-C. Cha, M.-S. Chuang, K.-H. Yeh, Z.-J. Huang, and C. Su, "A user-friendly privacy framework for users to achieve consents with nearby ble devices," *IEEE Access*, vol. 6, pp. 20779–20787, 2018.

[60] F. Ullah, M. A. Habib, M. Farhan, S. Khalid, M. Y. Durrani, and S. Jabbar, "Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare," *Sustain. Cities Soc.*, vol. 34, pp. 90–96, Oct. 2017.

[61] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

EMAN M. ABOU-NASSAR received the B.S. and M.S. degrees in computer science from Menoufia University, in 2010 and 2015, respectively. She has been a Assistant Lecturer with the Mathematics and Computer Science Department, Faculty of Science, Menoufia University, since 2016. She taught over 7000 hours of programming languages, Data Base, Data Structure, and other computer science courses. She attended the 3RD Africa and Middle East Conference on Software Engineering (AMECSE2017), December 2017, Cairo, Egypt, and IEEE 9th International Conference on Informatics and Systems (INFOS), 2014. She has four publications in fields of language semantics, the IoT, and blockchain. She is also engaged in many research projects on smart cities and the healthcare IoT systems.

ABDULLAH M. ILIYASU (AKA ABDUL M. ELIAS) (Senior Member, IEEE) received the M.E., Ph.D., and Dr.Eng. degrees in computational intelligence and intelligent systems engineering from the Tokyo Institute of Technology (Tokyo Tech.), Japan. Concurrently, he is a Research Faculty with the School of Computing, Tokyo Tech and also the Principal Investigator and the Team Leader of the Advanced Computational Intelligence and Intelligent Systems Engineering (ACIISE) Research Group, College of Engineering, Prince Sattam Bin Abdulaziz University (PSAU), Saudi Arabia. He is also a Professor with the School of Computer Science and Technology, Changchun University of Science and Technology, China. In addition to being among the pioneers of research in the emerging quantum image processing (QIP) subdiscipline, he has to his credit more than 100 publications traversing the areas of computational intelligence, quantum cybernetics, quantum image processing, quantum machine learning, cyber and information security, hybrid intelligent systems, the Internet of Things, 4IR, health informatics, and electronics systems reliability. He is the Managing Editor of Fuji Technology Press, Japan. He is a member of editorial board many journals including *Journal of Advanced Computational Intelligence and Intelligent Informatics* (JACIII), *Quantum Reports* journal, and the *Journal of Medical Imaging and Health Informatics* (JMIHI). He is also an Associate Editor in many other journals, including IEEE Access and *Information Sciences*.

PASSENT M. EL-KAFRAWY received the bachelor's degree from the Computer Science and Engineering Department, American University, Cairo, the master's degree from the Faculty of Science, Menoufia University, and the Ph.D. degree in computer science and engineering, in the field of computational geometry and artificial intelligence, from the University of Connecticut, USA, in 2006. She joined the Information Technology and Computer Science School, Nile University, in 2019. She has been a Professor, since 2018. Then she taught at Eastern State University of Connecticut for one year. In 2007, she has worked as an Assistant Professor with the Mathematics and Computer Science Department, Faculty of Science, Menoufia University. In 2011, she joined the Computer Science and Engineering Department, American University, as an Adjunct Professor. She has appointed as an Associate Professor in 2013. She has over 45 publications and editor in three books. She has been supervising several research studies between Ph.D. and M.Sc. in the field of natural language processing, semantic knowledge, bioinformatics, big data analytics, and knowledge mining and acquisition. She is a member of the Egyptian Society of Language Engineering and the Editor in Chief of the *Journal of Egyptian Language Engineering*. She has joined the IBRO School for neurodegenerative physician training organized by ENND and personalized medicine workshop organized by AUC. Her research interests include software engineering, bioinformatics, big data analytics, machine learning, and cloud computing.

OH-YOUNG SONG received the B.S., M.S., and Ph.D. degrees from the School of Electrical Engineering and Computer Science, Seoul National University, South Korea, in 1998, 2000, and 2004, respectively. He was a Postdoctoral Fellow with the School of Electrical Engineering and Computer Science, Seoul National University, from 2004 to 2006. He is currently an Associate Professor with the Department of Software, Sejong University, South Korea. His research interests include computer graphics, simulation, and machine learning. Especially, he has contributed in the areas of physics-based animation, human motion, numerical algorithms, VR/AR, medical image analysis, and deep learning.

ALI KASHIF BASHIR (Senior Member, IEEE) received the B.S. degree from UMT, Pakistan, the M.S. degree from Ajou University, South Korea, and the Ph.D. degree in computer science and engineering from Korea University, South Korea. He is currently with the School of Computing and Mathematics, Manchester Metropolitan University, U.K. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, National University of Science and Technology, Islamabad (NUST). He is a Distinguished Speaker of ACM. His past assignments include an Associate Professor of information and communication technologies with the Faculty of Science and Technology, University of the Faroe Islands, Denmark; Osaka University, Japan; the Nara National College of Technology, Japan; the National Fusion Research Institute, South Korea; Southern Power Company Ltd., South Korea, and the Seoul Metropolitan Government, South Korea. He has advised several startups in the field of STEM-based education, robotics, and smart homes. A few of these are RNS Solutions, Edvon, UHom, and Bandz Networks. He is the author of over 90 peer-reviewed articles. He is supervising/co-supervising several graduate (M.S. and Ph.D.) students. His research interests include the Internet of Things, wireless networks, distributed systems, network/cybersecurity, and cloud/network function virtualization. He has served as the (Program, Publicity, and Track) chair on several conferences and workshops. He has delivered several invited and keynote talks, and reviewed the technology leading articles for journals like the IEEE Transactions on Industrial Informatics, the *IEEE Communication Magazine*, the IEEE Communication Letters, the IEEE Internet of Things, and the IEICE Journals, and conferences, such as the IEEE Infocom, the IEEE ICC, the IEEE Globecom, and the IEEE Cloud of Things. He has been serving as the Editor-in-Chief for the IEEE Future Directions Newsletter. He is an editor of several journals and has served as a guest editor on several special issues in journals of IEEE, Elsevier, and Springer.

AHMED A. ABD EL-LATIF received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2005 and 2010, respectively, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology (H.I.T), Harbin, China, in 2013. He is currently an Associate Professor of computer science with Menoufia University, and the School of Information Technology and Computer Science, Nile University, Egypt. He is the author or a coauthor of more than 100 papers, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, and book chapters. His research interests include multimedia content encryption, secure wireless communication, the IoT, applied cryptanalysis, perceptual cryptography, secret media sharing, information hiding, biometrics, forensic analysis in digital images, and quantum information processing. He has many collaborative scientific activities with international teams in different research projects. He is a Fellow at Academy of Scientific Research and Technology, Egypt. He received many awards, the State Encouragement Award in Engineering Sciences, in 2016; the Arab Republic of Egypt; the Best Ph.D. Student Award from the Harbin Institute of Technology, in 2013; and the Young Scientific Award, Menoufia University, Egypt, in 2014. Furthermore, he has been reviewing articles for more than 85 international journals, including the *IEEE Communications Magazine*, the IEEE Internet of Things journal, *Information Sciences*, the IEEE Transactions on Network and Service Management, the IEEE Transactions on Services Computing, *Scientific Reports (Nature)*, the *Journal of Network and Computer Applications*, *Signal Processing*, *Cryptologia*, the *Journal of Network and Systems Management*, *Visual Communication and Image Representation*, *Neurocomputing*, and *Future Generation Computer Systems*. He is an Associate Editor of the *Journal of Cyber Security and Mobility*.

• • •