Secure Semantic Smart HealthCare (S3HC)

Sanju Mishra Tiwari[1,*], Sarika Jain[2], Ajith Abraham[3] and Smita Shandilya[4]

[1]*Terthankar Mahaveer University, Moradabad, India*
[2]*National Institute of Technology, Kurukshetra, India*
[3]*Machine Intelligence Research Labs (MIR Labs), Washington, USA*
[4]*Sagar Institute of Research Technology and Science, Bhopal, India*
E-mail: tiwarisanju18@ieee.org; jasarika@nitkkr.ac.in; ajith.abraham@ieee.org; smita.sam27@gmail.com
[*]*Corresponding Author*

Received 09 January 2019;
Accepted 13 March 2019

Abstract

Healthcare is a significant domain having a huge knowledge base, a significant part which comes from medical, diagnostic and imaging devices and sensors. The health status of patients may be monitored and managed remotely by performing reasoning over this knowledge base. Specialists in HealthCare facilities are required to handle large quantity of data generated and make decisions. However, the heterogeneous and complex nature and the huge amount of data generated; the way it is represented and presented; and the security challenges may overburden the core abilities of thinking and reasoning of even highly skilled and knowledgeable experts putting the lives of patients at risk. The situation may become even worse when data is coming from various healthcare devices and sensors which are themselves characterized by a number of representation and serialization formats. To address the various challenges in healthcare, this paper tries to represent and hence exchange the data collected by healthcare devices meaningfully and securely. This allows all healthcare devices to operate in conjunction with each other facilitating deeper insights and enabling generation of intelligent recommendations.

Journal of Web Engineering, Vol. 17_8, 617–646.
doi: 10.13052/jwe1540-9589.1782

To transfer the collected data from devices to the knowledge base and vice versa, a healthcare IoT ontology with sensors and actuators is developed. SPARQL queries and SWRL rules are composed to provide personalized services and alleviating the doctors' workload.

Keywords: Semantic Web, HealthCare, Ontology, Knowledge Base, SWRL Rules, Semantic Web of Things.

1 Introduction

The HealthCare organization environment consists of an array of institutions, organizations and people providing services as well as obtaining services at the same time. The idea of e-Health [1] is considered as a new thought for implementing a healthcare system based on internet communications and electronic mechanisms. A healthcare system includes clients, servers and devices [2]. Clients can be doctors, patients, guardians and, nurses who have the permission to access the systems through sensor attached devices such as specific health devices and mobile phones for monitoring the status of the patient, fetching health history and sensing data. An important part of this environment comprises of the health data provided by the healthcare IoT sensors and IoT devices. HealthCare information systems are significant application fields where IoT smart technologies are frequently applied to facilitate efficient solutions. The health diagnostic sensors and devices are effectively employed in hospitals to collect the patient data for the diagnosis, treatment and monitoring. For example, blood glucose meter, thermometer, heart rate sensor and blood pressure monitor are used for monitoring the patient health status. All categories of data acquisition instruments (sensors and IoT devices) can be associated with each other by using the Internet in multiple ways. IoT connects these scattered data acquisition instruments together effectively and provides a smart and connected HealthCare. A web-based healthcare system can be taken as the solution to provide healthcare services to the people in their everyday lives. It requires a regulation of care by secure and timely information sharing. A web based healthcare system demands to manage semantically generous and strongly structured health data in a heterogenous environment. Doctors can monitor their patients anywhere, anytime and can update prescriptions when needed.

These devices are web based and are able to monitor the health status of any patient remotely, but are not able to provide an integrated view of the various information collected because of the heterogeneity of the IoT devices and lack of common accepted standards. It is required to describe the rules and alerts under certain situation for querying, storage and analysing the collected health data from the sensors and devices. In this context, significant aspects are ensuring consistency, data sharing between devices and exchanging data between devices without losing its meaning. To achieve these, semantic web technologies are incorporated with IoT devices. The semantic web technologies and principles are greatly adopted as a solution to these interoperability issues, leading to the development of a new domain, the Semantic Web of Things (SWoT). The semantic web is accepted as an enrichment of the syntactic web where information is contained with its meaning. Semantic web consists of documents as well as data on the World Wide Web and hence machine can assemble, execute, and transform the data in an effective manner. For sharing and reusing data across heterogeneous applications and/or devices, semantic web provides a general framework. This framework is based on Resource Description Framework (RDF) that assimilates several applications, applying Extended Markup Language (XML) is accepted for syntax and a URI is considered for naming. Semantic web technologies are considered as promising tools for communicating with numerous smart devices having heterogeneous capabilities to share data and exchange their services precisely. SWoT empowers semantic-enriched ubiquitous computing by integrating intelligence into environments and general objects through a huge variety of distributed micro-devices, each transmitting a little volume of information. The Internet of Things (IoT) concept enables heterogeneous applications and devices to interact with each other for supporting autonomous and seamless services. Semantic web technologies need IoT-based solutions for delivering sensor based services and remote monitoring through association among entities and will provide comfortable and efficient services to the end users. The IoT paradigms and semantic web are emerging more and more toward and referred as Semantic Web of Things (SWoT) [3, 4].

Researchers are harnessing the power of SWoT in HealthCare, but still there is a need to ensure privacy and sensitive information [5]. The semantic models correctly includes all terminology of healthcare and their relationships to existing models for inducing health messages, but still needs further pragmatic evaluation to improve the security for semantic interoperability. Semantic technologies have been effectively applied to alert

the heterogeneity challenge to (i) infer new knowledge to design smart applications and (ii) associated health domain data (iii) control interoperability at data processing, storage and management. These requirements comprise security challenges such as data integrity, confidentiality, trustworthiness, authentication, authorization and access control within the IoT network, the enforcement of privacy and security policies, trust and privacy among users and objects. These security challenges can be obtained by integrating semantics and reasoning engine in amenable devices. SWoT devices can be integrated from different domains in a healthcare environment to assist Physicians and patients remotely.

1.1 Issues and Challenges in Semantic Web of Things

Exploiting SWoT involves various issues such as:

- The enormous use of IoT devices produce big data.
- This big data is hererogeneous in source and format, so badly represented, misunderstood, and under-utilized by devices and systems.
- The large amount of IoT devices are associated to devices like sensors, actuators, RFIDS, etc. which are resource-constrained.
- Annotation of available resources
- Semantic connection / association, activation and analysis of these resources

The challenges involved are:

- Security and Privacy: The IoT devices produce sensitive context rich data, thus providing threat to data confidentiality and privacy. It is essential to ensure the functioning of connected objects and to assure an adequate and valid identified information.
- High Computational Power: The enormous heterogeneous data captured by sensors and devices are required to be converted into high level abstraction which demands for high end processing abilities.
- Representation and Reasoning: The semantic description of both associated objects and their information is required to be defined in order to allow data to be universally understandable. The semantic reasoning of this data needs to define the distinct rules in order to achieve adequate and efficient results.
- Ensuring IoT scalability and flexibility: The sensor data can be accessed in a scalable way through standard semantic services.

- Standardization of IoT interconnected devices: Standards are required for data formats, data models and ontologies
- Data Quality: The Web of Data model contains innovative aspects focusing on data quality.

1.2 Hypothesis and Results

IoT devices are not interoperable with each other; they do not utilize general facts or vocabulary to express the interoperability of IoT data. Exploiting, enriching and combining this data to develop smarter interoperable applications is becoming a great challenge. The semantic technology utilization does well in resolving the issue of interoperability among IoT devices [6]. Several semantic models [7] are introduced for describing the physical objects using Description Logics and ontologies to enable semantic interoperability. This does not come without an associated cost. When two objects communicate with each other; due to lack of safe communication link, data can be stolen or manipulated (privacy), channels can be breached. The semantic models for semantic interoperability needs proper identification and authentication to enhance the semantic security for heterogeneous devices and physical objects.

In this paper, author introduced a secure semantic smart model for healthcare domain to perform the monitoring of end users and maintain security such as: authentication, integrity and confidentiality, etc. We have presented a semantic model with security layers interconnected with IoT devices. The major contributions of this research are as follows:

1. Present a Secure Semantic Web of Things framework with ontology representation and reasoning to address the various challenges in healthcare.
2. Represent the knowledge gained and data gathered from the IoT healthcare devices and sensors semantically into a HealthCare IoT Ontology (HCIoTO). Any existing healthcare ontology can embed this ontology and can interact with IoT devices. This ontology will collect knowledge about the health status, threats and alerts and facilitate reasoning power to identify implicit information from the contextual information.
3. Accessing and exploiting this semantic representation in order to provide the investigation of the vital signs and diagnosing the patient using SPARQL queries and SWRL Rules.
4. Maintain the security in IoT based health devices such as blood glucose meter, thermometer, heart rate sensor and blood pressure monitor.

1.3 Evolution of Things

Cyber-physical system is a concept where humans are interacting with the machine to share the information globally. In every field today, it is required to connect people with machines to make smart and intelligent life. Three major things are discussed in this section.

- **Internet of Things (IoT)**
  IoT is a collection of associated physical objects network such as vehicles, devices, sensors, software and connectivity of networks that promotes these objects to gather and share data without demanding human-to-machine or human-to-human interaction.
- **Web of Things (WoT)**
  The Web of Things (WoT) an enhancement of IoT and represented as a part of the major activities in the IoT applications. WoT leverages the Web to be successful and implementing their methods to the physical objects. It makes possible that the development of data and IoT can be usable to a huge amount of Business and Web designers thus reusing the knowledge available on the web to enrich the IoT applications.
- **Semantic Web of Things (SWoT)**
  SWoT is an integration of web based IoT applications and semantic web technologies to improve the data and enable its significance in diverse and multiple applications and termed as "Semantic Web of Things" (SWoT). It is domain independent; data will be produced by one domain and applied in heterogeneous domains. An open data portal is the best example, here data is proposed to any developer making use of it and data format is described and simply generic, thus several applications may be designed.

The rest of the paper is framed as: Section 2 discusses related work. Security Issues in Semantic Web of Things are discussed in Section 3. Our semantics framework for smart and secure healthcare is discussed in Section 4. Section 5 presents a simulation environment with a case study for healthcare where HealthCare IoT ontology has been developed and reasoning performed over it. Finally, the conclusion and future possibilities are drawn in Section 6.

2 Related Work

In [7], the authors introduced a semantic model to describe the smart objects by using description logics and ontologies to promote Semantic Interoperability among the agriculture domains. To digitize agriculture domain, it is required

to gather the information about irrigation decisions support and crop growth monitoring based on smart objects.

To make use cases for digital agriculture, Jayaraman et al. [8] described an OpenIoT platform. This OpenIoT platform applied ontologies to represent domain concepts of Phenonet for collecting smart collection of information, validation and annotation tasks to promote the semantic based interoperability. An intelligent and scalable IoT architecture is in demand for future era to promote the analysis of physical sensors and their syntactic and semantic interoperation.

Desai et al. [9] introduced a Semantic web enabled framework to provide interoperability among various smart objects. To make an interpretation between IoT protocols such as CoAP, MQTT and XMPP, semantic web technologies are integrated with the Semantic Gateway as Service (SGS). For semantic reasoning, ontologies are applied to deliver Semantic Interoperability among different communicating messages. For semantic interoperability with IoT devices, several approaches are designed.

Intelligent Personal Assistant (IPA) is used as software agent by the author [10] in IoT device for doctors to provide real time information of the patients under observation. The information is collected by the AMBRO mobile gateway from various IPA devices and then proceeds required action. It facilitates interoperability among various IPA devices.

Linked Open Vocabularies for Internet of Things (LOV4IoT) is considered as a dataset for different relevant domains such as weather, smart home, agriculture and healthcare [11]. This dataset is referred by almost 300 ontology-based domain-specific projects in several domains. These domain ontologies are categorized based on their status, such as online, not available following real practices. Although it is accepted, but it has some limitation such as it needs to work manually not able to perform automatically.

Bandyopadhyay et al. highlighted the secure IoT architectures at the development phase [12]. Alam et al. highlight the IoT security reasoning through semantic rules and ontologies and they discussed security challenges for IoT such as integrity, confidentiality, authorization, authentication, trustworthiness, access control, etc [13]. But they do not discuss which security processes we should combine in own IoT systems.

Semantic web technologies, offer various benefits to IoT and WoT including; a) for unifying heterogeneous data and metadata are explicitly expressed, there are sensor datasets for semantic annotation; b) enhancing semantic sensor datasets with their external knowledge graphs and; c) representing analytics on the data by means of reasoning process and applied logic to infer fruitful additional information.

2.1 Semantic Web in Healthcare

In intelligent healthcare systems, ontologies are used for the purpose of semantically analyzing user's health data. In such systems, users can use services at anytime, anywhere and also maintain privacy. The system returns responses to the users and the care provider.

A clinical decision support system (CDSS) has been designed by Galopin et al. in [14] for the patient management with several chronic disorders. They have presented reasoning and an ontological modelling for the contents of clinical practice guidelines.

Sherimon et al. [15] have presented a system called Onto Diabetic to analyze the risk factors and to facilitate proper treatment for the patients of diabetes. They imply OWL2 rules for the implementation and modelling of clinical guidelines and the reasoning task of the Onto Diabetic system. But these works have various issues; they are based on clinical practice guidelines and patient medical record without having new technologies as IoT, SWoT in the healthcare domain.

Semantic models can be applied for various purposes such as rules description, information representation, and to filter or cluster the data [16]. Zhang et al. propose a semantic model to describe the designed healthcare rules for fixing the alarm conditions by observing the sensing data from healthcare sensors such as lipid, heartbeat and blood pressure [17]. Sezer et al. propose the semantic model for the healthcare system by specifying the device and domain information along with describing rules to facilitate suitable services [18].

Several expert systems for health care have been proposed such as; expert system for diagnosing the breast cancer [19], a rule-based solution to assure patient safety at the time of breast cancer surgery [20] that applies semantic web techniques, a system for enhancing alarms specificity in critical care environments [21], a hybrid approach [22] using rule-based reasoning and case-based reasoning for decision support in ICUs, and an antidiabetic drugs selection recommendation system [23].

3 Secure Semantic Web of Things

Several IoT devices are used in healthcare domains such as blood glucose meter, thermometer, heart rate sensor and a blood pressure monitor. These smart devices are lack in interoperability at the application level, they are required to improve for remote monitoring, semantic reasoning and representation. WoT and IoT devices are not capable to represent the critical

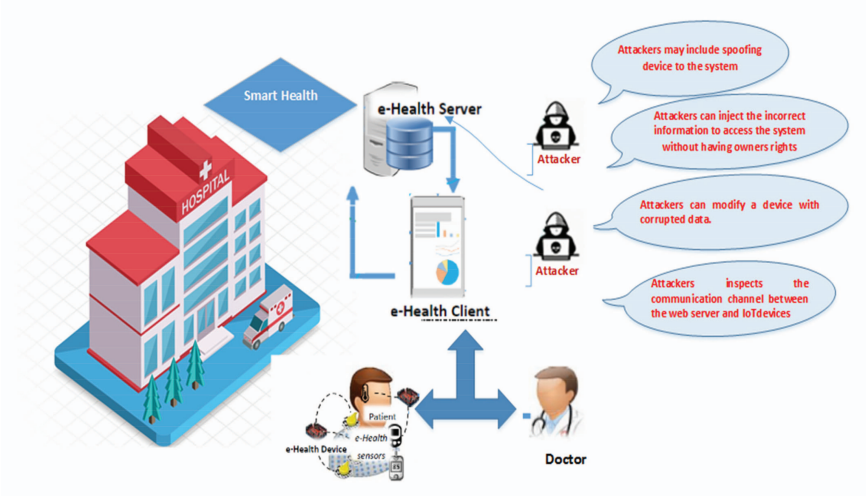

Figure 1 Smart healthcare without semantic remote monitoring.

relationships between human and machine. Both technologies are failing during semantic collaboration and dynamic decomposition. The HealthCare IoT devices do not have security features, for eg. tomography scanners provide measured radiation, but they can be damaged and may create threatening to life. The unencrypted and unauthenticated communication are also major vulnerabilities and can disturb the health devices remotely. In Figure 1, we can see a smart heathcare system with IoT devices but without semantics involved. We can see here that how an attacker can make threats on e-Health Server and clients.

An attacker can perform the following vulnerabilities:

- It can include a spoofing device to the system.
- It can inject the incorrect information to access the system without having owners' rights.
- It can modify a device with corrupted data.
- It inspects the communication channel between the web server and smart devices.
- It can leak the secure data to unauthentic users during diagnosis.
- It can disturb the smart device control system during transmitting the prescriptions of doctors.
- It can steal the confidential records of patients from the storage.

Lacking of awareness of the security problems, and weak security aspects generate the underlying implication of mixed health security programs in device monitoring and interpreting messages. These poor practices comprise lack of secure devices disposal that consist data, password sharing and password distribution specifically in devices where passwords are needed for device access. Some strong security challenges and interoperability issues are discussed in Sections 3.1 and 3.2.

3.1 Security Challenges in SWoT

SWoT has several security issues, it may damage and threaten human lives and devices in healthcare domains. To enhance the abilities of providing emergency response, monitoring, and predicting the designing trend of IoT security, we have highlighted some security challenges that need to fix:

- **Confidentiality:** SWoT services can have sensitive data; for protecting the data of IoT connected objects, it should be stored confidentially. By the encryption process, one can achieve confidentiality. For ensuring confidentiality there are several existing asymmetric and symmetric encryption schemes. However, choosing of a specific type of encryption is extremely device and application ability dependent. For example, consider a healthcare environment that handles the information about the patient activity at the hospital. The doctor will never wish that anyone in hospital will access the data by monitoring devices of patient activity.
- **Integrity:** IoT services interchange crucial data with other services and also with the third parties that keeps forward rigorous demand that stored, sensed and transferred data should not be damaged either accidentally or maliciously. To protect the integrity of sensor data is critical for developing dependable and reliable SWoT applications. It is assured, with message authentication codes (MAC) applying one way hash functions. The choice of MAC technique also depends on device and application capabilities. For example, smart home that is linked with the smart grid. For producing electricity bill, this smart grid offers a monitoring of electricity consumption. The provider never welcome that the consumed data can be damaged during the transmission period.
- **Availability:** Our anticipated SWoT environment can consist of sensor node hosted services. Hence, it is highly significant that these services exist from everywhere at any time in order to produce semantic based information. To satisfy this property, there is no security protocol. However, various pragmatic measures may be accepted to assure the availability.

- **Authentication:** It is applied to the identity verification. In SWoT term, mutual authentication is required because SWoT data are applied in actuating processes and decision making. Therefore, the service consumer and the service provider need to be ensured that the service is approached by an authentic service and a user is provided by an authentic source. Applying any authentication process requires to register the identities of user and resource issues of SWoT objects causes restrict constraints to empower the technique of authentication.
- **Authorization:** It is applied to describe the access policies that usually appoint certain privileges to subjects. The SWoT environment requires facilitating re-useable, fine-grained, dynamic, updating, and easy to use policies describing mechanism. Hence, it is significant to externalize the definition of policy and enforcement process of SWoT services.
- **Access Control:** This is considered as an enforcement process that permits access to the resources for only authorized users. The enforcement is generally based on the outcomes of the access control. It is highly significant to reveal users' data only to the authorized parties.
- **Trustworthiness:** Several applications that are delicate in nature, such as healthcare services, safety critical services, require to analyze trustworthiness of various entities indulged. From a SWoT application perspective, analyzing trustworthiness of sensors data and sensor is significant. Non-trustworthy sensor data or malicious sensor nodes can lead to a disaster in safety critical places. Untrusted sensor data can enter from a trusted sensor node. Non-trustworthy nature can have two reasons: unintentional errors and intentional misbehavior. It can be easier to assure trustworthiness of SWoT by incorporating trustworthiness analysis.

3.2 Interoperability Issues in SWoT

Interoperability is considered as the ability of heterogenous systems to interchange data and applied information. This feature presents several challenges on how to obtain the information, use the information and exchange data in understanding it and being able to process it. Interoperabilities [25] are classified into four categories:

Technical interoperability employs heterogeneous hardware and software (e.g., heterogeneity of communication protocol).

Syntactical interoperability employs data formats (e.g., XML or JSON). Syntactical interoperability is also an issue for reusing and combining semantic

datasets or ontologies designed with unique software dealing with unique syntaxes (e.g., XML/ RDF, N3).

Organizational interoperability employs heterogeneity of the various infrastructures.

Semantic interoperability employs (a) ontology heterogeneity (b) terms used to express data (c) the meaning of content interchanged according to the context. This is significant to later translate Internet of Things data and construct interoperable semantic-based Internet of Things applications.

The primary challenges that are notified in Semantic Interoperability and needed research in future include:

- Data Exchange and Data Modelling and
- Ontology matching/merging & alignment
- Semantic Annotation for Data/Event
- Knowledge Representation and associating ontologies
- Sharing of Knowledge
- Knowledge Consistency Revision
- Reasoning & Analysis

3.3 Security Issues in SWoT

The more accurate model can be designed by the semantic analysis of data in SWoT for diagnosing the privacy and security issues. These issues are significant in different areas like Information Processing, Gathering, Invasion and Dissemination. In this section, we try to include the distinct security challenges represented in a SWoT environment and simplify issues from a security aspect that are connected with computing applications, devices and networks. The concepts of security and privacy are identified and certain security requirements are noted. In IoT applications, there are several categories of security incidents. These incidents are discussed in Table 1.

Table 1 Listing of SWoT security incidents

Incident Category	Incident Type
Information Security	Unauthorized Deletion/Access/Updation
Fraud	Wastes of Resources
Information Collection	Phishing, Sniffing
Malware	Infection, Undetermined
Availibility	DoS/DDoS

Information Security (Unauthorized Access) consists the majority of security problems for access control in SWoT applications. Various access control frameworks are there that are formed upon SW languages (RDF, OWL, SPARQL) for preventing their resources from unauthorized access. SW languages support enforcement policies and designs access control policies. For restricting access to RDF data, the IS category also provides encryption techniques. As encryption is considered as the cornerstone of information security, hence authorized encryption getting enough attention in the SWoT context to promote integrity and confidentiality. Lightweight and fast encryption plays a significant role in acquiring the adapted security and privacy for IoT. Ontologies [26–28] are considered as an interesting area for IS as a basis for detecting and analyzing security issues. Ontologies are generally applied as representation schema, knowledge bases, or an annotation vocabulary. Infection analysis or malware detection is considered as knowledge intensive security issues. Fraud, Information Collection, Malware and availability are another common security area such as phishing or SPAM.

4 Secure SWoT Representation and Reasoning Framework for Healthcare (S3HC)

Several researchers have done work in this direction, but still there is a need to improve certain issues like the security of semantic web in collaboration with its devices in healthcare systems. According to the literature, there is less attention to make secure SWoT for health devices. As we have discussed in Figure 1, there are no semantic web layers between the web based IoT applications and end users. Information can be accessed without any security protocols. Any end user can access the information and this information can be easily tampered by attackers. Several devices like blood glucose meter, thermometer, heart rate sensor and blood pressure monitor are applied for treating and monitoring patients. Attacker aims to exploit vulnerabilities in healthcare devices attached to the network and usually targets: database servers, application software and web servers.

1. **Database servers:** Several systems and devices have a data store or database to retain information for that device, usually referred to as a database back-end. Most of them use form of structured query language (SQL), and they are greatly vulnerable to SQL injection. The SQL injection is a serious type of attack, which degrades all security challenges (confidentiality, availability, and integrity etc.). The attacker can damage

all information stored in the database, inject corrupted data which loss integrity and can read the information that generates a confidentiality breach.

2. **Application software:** It deals with running software on a healthcare device. These attacks are generally successful where software has not been tested to determine the existing vulnerabilities. Attackers exploit vulnerabilities in source code of applications that do not properly tested prior to deployment.
3. **Web servers:** For interfacing with health devices, web based applications are quite common to provide a graphical user interface that connects the end users. But these interfaces are having vulnerabilities exploited by an attacker. Several attack tools are freely available to use and download that can scan the interfaces and outline the vulnerabilities if present in the web service. Attackers can apply this information to build a particular payload for attacking a vulnerable target.

We present a secure semantic web of things model to represent the IOT resources and data and to reason within healthcare systems. This Secure-Semantic-Smart HealhCare (S3HC) framework is depicted in Figure 2. It comprises of four components, namely the knowledge base, the secure semantic web layer cake, Services and Data Processing and the end users.

4.1 Knowledge Base

A knowledge base contains all the concepts and properties (aka terminology, TBOX) and all the instances (aka assertions, ABOX). The content of a knowledge base forms an ontology containing the terminology and the assertions from which reasoning and querying can be done. Ontologies are essentials for interoperability between systems. For obtaining full interoperability, the semantics of information have to be the common for all systems. Ontology presents format as an explicit specification of a conceptualization [25]. Ontology can be managed by the devices and expresses the definitions of framed concepts and restrictions on possible interpretations among these terms to build a structure on the domain and how these concepts are connected to each other. The ontology applies the reasoning power to diagnose the knowledge base correctness, uniformity of assertions and data individuals using rules. This process extracts implicit facts from the available knowledge and can be categorized into rule-based reasoning, logic-based context reasoning or inductive or deductive reasoning.

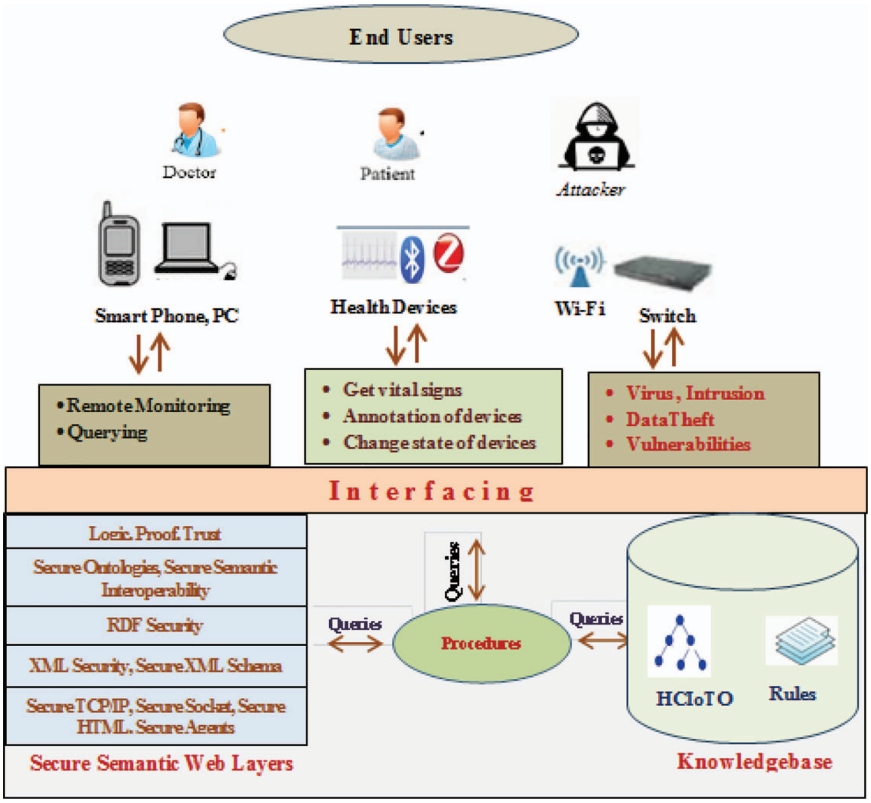

Figure 2 Secure Semantic Smart HealthCare framework (S3HC).

The patient information will be stored in the form of RDF-graph and SWoT-O vocabulary as a knowledge base. The entities such as concepts, attributes, properties and relationships between entities are kept in RDF graph and finally stored in the Knowledge base. To fetch this information securely SPARQL query or rules are used to get the authentic data. It provides semantic search and reasoning which is based on logical rules or statistical methods. These rules are framed on SWRL, Jena rules and Jena API with reasoner. All confidential information of health domain, such as patients, doctors and devices is stored in the knowledge base (KB) in the form of ontology. To interact with the KB, it is required to write the queries and SWRL rules. These queries and rules will be interpreted by inference engine or semantic reasoner such as pellet, racer, fact++ etc. These reasoners interpret the meaning of the request sent by end users. It checks the consistency, accuracy, correctness

of requested data if it is logical and related to the domain then it returns expected results otherwise it will not respond to the end users. Resource Description Framework (RDF) is presented as a semantic web framework and used to connect things using triples to create it semantically meaningful. To make semantically interoperable of patients' data, RDF annotation has been applied. SPARQL query is framed to obtain records from RDF graph. But for complex restriction, OWL and SPARQL are lacking in its expressivity. In OWL it is difficult to express the relation between individuals with other individuals. To overcome with these situations rules are used to improve the expressivity and discover the hidden relationships in ontology. Rules are perfect for generating the active knowledge design the design support tasks such as an alerts, recommendation and guidelines in the healthcare domain. Ontology and Rules build a knowledge base for any specific domain.

4.2 The Secure Semantic Web Layer Cake

The secure semantic web layered stack sits as a glue along with all the procedural knowledge. In this stack, at the lowest level, the semantic web has the protocols TCP/IP, SSL, HTTP. These protocols are used for data transmission and helps to transmit the web pages over the internet. These protocols do not focus on syntax and semantics of web documents. Documents are not marked up for a standard representation, which are transmitted by using these protocols. To overcome this problem, XML and XML Schema layer are included. Both are standard representation languages for exchanging documents. XML provides a uniform representation for document exchange. XML Schema expresses the XML document structure. But an XML document can have different interpretations on different sites because they focus only on syntax. To express the concepts with semantics, at level 3, RDF (Resource Description Framework) is introduced with security. Secure semantic interoperability is handled at level 4. The topmost layer represents logic, trust and proof.

4.3 The End Users

There are three types of end users that usually access the smart devices; doctors, patients and attackers. Doctors can use smart devices to monitor their patients remotely from any location to send the prescription for daily monitoring. Patients can use the smart devices to send their health status and complaints to get the correct treatment from the doctors. In spite of doctors and patients

one more end users, attackers can access the smart devices to perform the threats within the system such as unauthorized access, damage the sensitive information, code injections and sniffing.

4.4 Services and Data Processing

Several services are discussed to achieve the goals of proposed framework such as:

- **Semantically annotating IoT data**
  Enriching devices and services with semantic annotations to qualify them as Semantic Web of Things. The connected objects, i.e., the IoT based health devices such as blood glucose monitor, heart rate sensor and blood pressure monitor are usually self-described with annotations containing their semantic description. They form the physical layer (layer 1) of the framework and the starting point of any analytics. Layer 2 consists of As soon as an instance of a connected object is discovered, the annotations are published to the system. Once gathered by the system, the semantic descriptions are stored in the knowledge base (HCIoTO+Rules).
- **Semantic Reasoning (Interpreting IOT data)**
  Authorized Doctors and Patient can perform semantic reasoning by using semantic web oriented IoT devices. There are several reasoners (Pellet, Hermit, Drools) are available to interpret the IoT data semantically. A doctor can reason to confirm about the diseases based on the collected symptoms by patients.
- **Data Integration and Fusion**
  A ontology (HCIoTO) is developed to integrate the health care information and IoT device information. Any existing ontology can merge this ontology to use sensors and actuator for the information fusion. This ontology also stores the information of IoT devices that are connected with the end users.
- **Getting Vital signs of the patient**
  The proposed framework is helpful to get the vital signs of the patients and decide the correct treatment to be taken. For example, if a patient has symptoms of Fever, then doctor can remotely monitor the patient for medicines and required test. On the basis of the doctor's recommendation the state of devices can be changed. Doctor's can successfully monitor their patients from any location.

- **Querying the knowledge base**
  To reason over the KB an inference engine is required to expose the hidden relationships. There are some common reasoners are available as an inference engine to reason over the KB such as Hermit, Fact++, RacerPro, Pellet. We have chosen Pellet to run the rules. Semantic Web technologies, achieving increased maturity in health systems to make more interoperable. Our knowledge, as there are several healthcare ontologies available such as FMA, MeSH, SNOMED-CT and NCI. These ontologies are developed by using OWL. To extend the stored knowledge of ontology none of these ontologies used SWRL rules [28].
- **Monitoring and Actuating**
  Monitoring involves detecting possible intrusions, ransomvares, viruses, data stolen. Monitoring tools provide information regarding various security alerts that are then diagnosed using different security tools, such as firewalls, vulnerability scanners, intrusion detection systems, etc. After gathering the data from sensors, it is required to make the decisions. Actuating involves performing the decisions that need to be taken. Actuating also involve for adaptation of existing services.

5 Simulation Environment

The semantic web is considered as a distributed environment where information is self-descriptive by means of machine understandable and well-described semantics. We collect the healthcare domain knowledge and create domain ontology. Some use cases pertaining to diseases are formalized. Then we write rules for realizing these use cases. Figure 3 shows the flow during the simulation depicting the five phases carried out.

5.1 Domain Information Collection

We develop a Healthcare IoT Ontology (HCIoTO) as part of simulating the architecture of S3HC. To develop any ontology, the first task is identifying the boundaries and its domain for representation.We are working in the domain of HealthCare, so the terminology and concepts pertaining to HealthCare need to be finalized. The HCIoTO has several concepts, relations, and instances of the healthcare domain.

For collecting the terminology, we discussed with two domain experts of GeneralOPD and represented this ontology for health domain which has

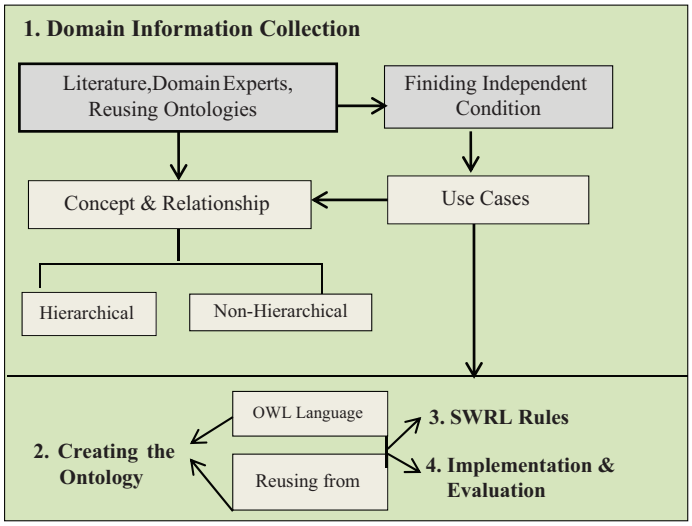

Figure 3 Simulation environment.

several concepts, relations, and instances of medical domains. We have designed some use cases to collect the concepts. For example:

UseCase 1: Dengue is caused by DengueVirus and it directly degrades the platelets of human body.

Terms: Dengue, DengueVirus, Body, Plateletes

Relations: caused_By, has_Symptoms()

UseCase 2: Tuberculosis is caused by Bacteria and affects on lungs of human being.

Terms: Tuberculosis, Lungs, Bacteria

Relations: caused_By, affects_On ()

Some of the concepts and relationships identified in this phase are summarized in Table 2.

For semantic representation of the associated objects and their data two type of knowledge need to be stored

- The contextual knowledge connotes terms qualifying the device in its environment (aka context aware applications) gathered from sensors. For example, its location, its acceleration, etc. This type of knowledge can be connected to individuals, properties and their values.

Table 2 Domain information

Concepts				Relations	
Staff	Doctor	Treatment	Surgery	Has	Cared_by
Nurse	Surgeon	Symptoms	Headache	Cares_for	Treated_by
Patient	Physician	Diagnosis	Fever	Looks_for	Operates_by
Device	Heartbeat	Sensor	BloodPressure	Operates	Transfer_data_to
Lungs	Dengue	Platelets	Virus	caused_By	affects_On
BonePain	MusclePain	Diagnosis	Manager	hasSymptoms	has_Events

- The structural knowledge connotes terms qualifying the intrinsic properties of the device and the resources. For example, its category, its size (Thermometer, blood glucose meter), etc. This knowledge can be connected to concept properties and their values.

5.2 Developing the Ontology

All collected concepts are classified as classes, subclasses, object properties, data properties or instances. The concepts are bound together into hierarchical and non-hierarchical relationships. Several healthcare ontologies are available, but it is inconvenient to reason over IoT devices for real-time decision support. The HCIoTO can be merged with existing ontologies and makes it easy to communicate with IoT devices to cope up the issues with existing healthcare ontologies. Protégé tool is used to frame these concepts into ontology and OntoGraph is used to visualize in a graph structure. Figure 4 represents a common ontology with sensors to interact with IOT devices like BP Sensores.

5.3 Writing the SWRL Rules

SWRL rules are used to find hidden information between individual. The use cases discussed in step 1 and collected concepts and relationships are used in the ontology treated as the blueprint for writing SWRL rules. We have modeled 20 rules. Some rules are discussed in Table 3.

5.4 Evaluation and Results

The term evaluation comprises the terms validation and verification [26]. Validation guarantees about the ontology that it responds to the system while verification refers to the technical process that guarantees the completeness, correctness and consistency. In order to solve and detect incompleteness,

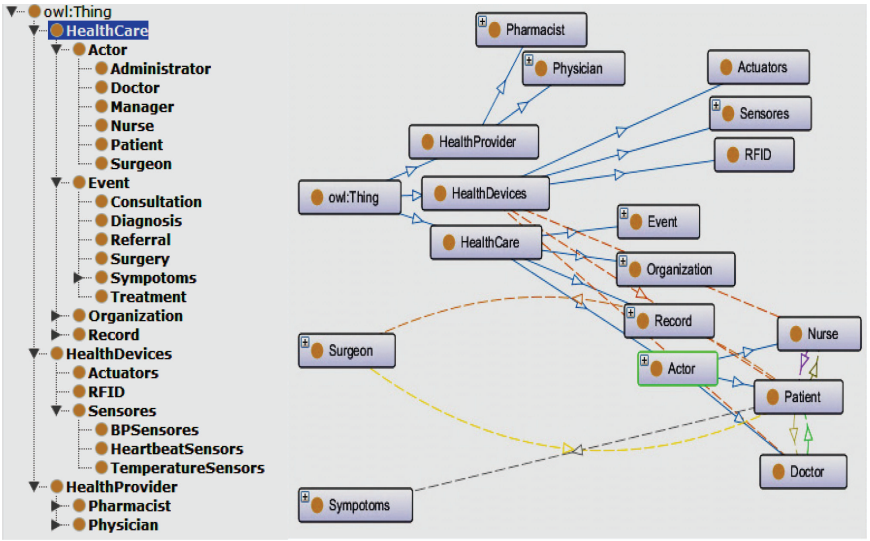

Figure 4 HealthCare IoT Ontology (HCIoTO) (a) Tree View (b) Graph View.

Table 3 Rules for HealthCare

S.N.	Description of the Rule
Rule 1	*Patient(?X)^hasSymptoms(?X, Fever)* → *Do_Test (?X, Malaria)*
Rule 2	*Patient (?X)^hasSymptoms (?X, Fever)^hasSymptoms(?X, BonePain)* → *Do_Test(?X, Dengue)*
Rule 3	*Patient(?X)^hasSymptoms(?X, MusclePain) ^hasSymptoms(?X, Inflammation)* → *Do_Test (?X, ESE)*
Rule 4	*Person(?X)^hasSymptoms(?X, Fever)^hasSymptoms(?X, BonePain)* → *Patientof Dengue (?X)*
Rule 5	*Patient(?p)^HealthDevices(SmartBP)^has_Sensors (?p, SmartBP)^BloodPressure(?b)^diagnose(SmartBP, ?b)^has_Value (?t, ?v)^swrlb:greaterThan(?v, 180)* → *has_Events(?p, HeartAttack)*
Rule 6	*Patient(?p)^has_event(?p, Dengue)* → *has_risk(?p, Death)*

redundancies, inconsistencies, we have examined the developed ontology and modeled rules for the requirement specification. Rules are formed to extract the hidden knowledge between the entities and presents accurate knowledge. Knowledge stored in the knowledge base is needed to verify for analyzing the accuracy of knowledge, because inaccuracy can result many security issues

for the whole system. Some competency questions are formed to examine the accuracy and completeness of the rules. These rules are successfully runs on Drools engine. SPARQL queries are modeled to run several competency questions. Some examples of questions are given here such as:

CQ1: Identify all the patients who have Symptoms of Muscle Pain and Inflammation disease and identify medical conditions.

CQ2: Identify patients who require regular Blood pressure monitoring.

CQ3: Identify all connected objects for the health status monitoring.

We have manually added patient cases to the knowledge base for executing SPARQL queries and rules. We have questioned total 30 questions from the HCIoTO. An example is shown in Figure 5 with its snapshot of running output in protégé.

It is required to verify the functioning of associated objects to assure a valid and accurate diagnosed data. With semantic annotation in Health IoT devices, there are less chances of frequent data access and data stolen. Any unauthorized user cannot access the information from the knowledge base. Only domain experts with access rights can access the information of patients and doctors.

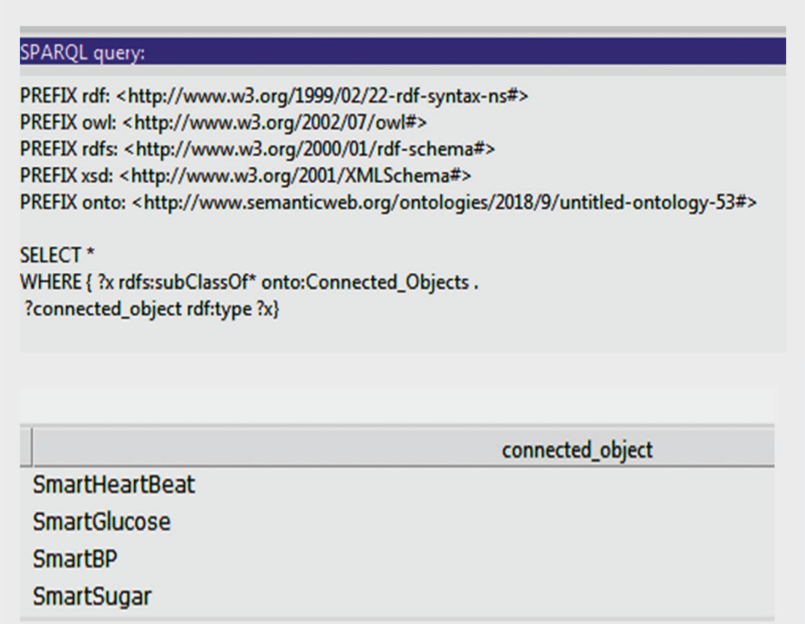

Figure 5 Reasoning with Ontology.

For example, if anyone wants to see the list of connected healthcare devices in the knowledge base, it is required to run the SPARQL query as in Figure 5 and it will display the result. XML Security and RDF Security protect the information stored in the knowledge base. We have tested 10 authorized users and 10 unauthorized users, who attempts to access the health information from semantic knowledge base. The evaluated metrics are shown in Table 4.

In Table 4, 30 SPARQL queries are tested and 20 Rule modeled in the knowledge base. Here 30 SPARQL is executed successfully by authorized and 20 rules modeled in the knowledge base. While unauthorized users have no access to get the information and notified as unknown users. We have compared our proposed model with existing models by analyzing some parameters in Table 5 and results are shown by the graph.

Table 4 Evaluation metrics

Users	No. of Users	SPARQL	Rule	Remarks
Authorized	10	30	20	Run Successfully
Unauthorized	10	No Access	No Access	Unknown Users

Table 5 Comparison table

Parameters Availibility	SWoT4CPS [29]	IoT-based HCIS [18]	HCIoT [30]	OB-CPS [31]	S3HC [Proposed Model]
Rule-based System	X	√	√	√	√
Access Control	X	X	X	X	√
Semantic Representation	√	X	X	X	√
Semantic Annotation	√	X	X	X	√
Integration and Fusion	√	X	√	√	√
Analysis and Reasoning	√	X	√	√	√
Visualization	√	X	X	√	√
Security and Privacy	X	√	X	√	√
Ontology Editor	√	X	X	√	√
Sensor Objects	√	√	√	√	√
Complex Relationships	X	X	√	√	√
Taxonomy Modelling	√	X	√	X	X

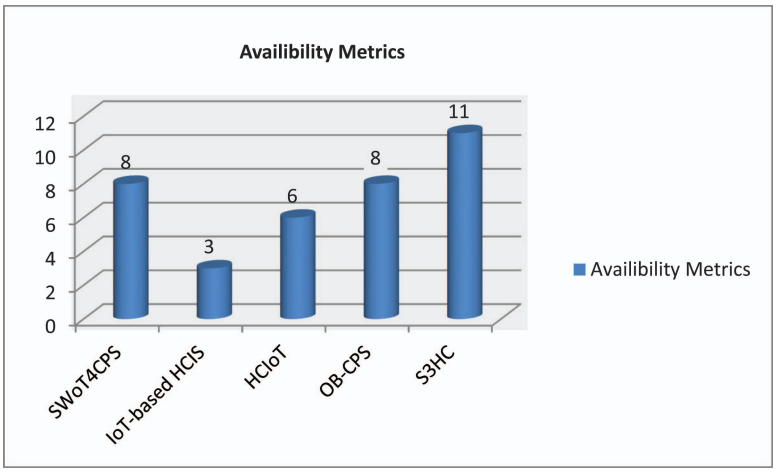

Figure 6 Availibility metrics of models.

In Table 5, we have analyzed 12 parameters among the existing models and proposed model. As we have examined, in *SWoTCPS* model only seven parameters are available, in *IoT-Based HCIS* model only three parameters are available, in *HCIoT* model only six parameters are available, in OB-*CPS* model only eight parameters are available but in our proposed model we can see that total eleven parameters are available. We have shown results in following graph.

6 Conclusion

This paper proposes to harness the power of the Internet of Things (IoT) and Semantic Web to transform HealthCare. IoT is seriously applied in the healthcare domain and generates a huge quantity of healthcare connected devices. Hence an enormous quantity of data is gathered, which carries several semantic interoperability challenges. In this paper, we have represented the collected data meaningfully and securely to address the various challenges. The S3HC framework supports doctors in analyzing the collected vital signs and in providing an appropriate and secure service for patients. To achieve our goals we have designed a healthcare ontology HCIoTO for transferring the collected data from the device to the knowledge base and vice versa. We have designed rules and run SPARQL queries to represent the accuracy and correct semantic reasoning between patients and doctors. The proposed model

has been compared with existing models and results are drawn to analyze the functionality of the model. Future works we will focus on guarantee the scalability of the proposed framework by reducing its response time when the amount of data and the number of rules increase.

References

[1] V. Della Mea, 'What is e-Health (2): The death of telemedicine?' J. Med. Internet Res., 3, e22, 2001.

[2] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, F. Wu, 'IoT-Based Smart Rehabilitation System'. IEEE Trans. Ind. Inf., 10, pp. 1568–1577, 2014.

[3] F. Scioscia & M. Ruta, 'Building a Semantic Web of Things: issues and perspectives in information compression'. In Semantic web information management (swim'09). in Proc. of the 3rd IEEE Int. Conf. on Semantic Computing, pp. 589–594, IEEE Computer Society, 2009.

[4] D. Pfisterer, K. Romer, D. Bimschas, H. Hasemann, M. Hauswirth, M.Karnstedt, C. Truong, 'SPITFIRE: Toward a Semantic Web of things', Communications Magazine, 49(11), IEEE, pp. 40–48, 2011.

[5] Y. Qin, Q.Z. Sheng, N.J.G. Falkner, S. Dustdar, H. Wang and A.V. Vasilakos, 'When Things Matter: A Survey on Data-Centric Internet of Things', J. Netw. Comput. Appl., 64, pp. 137–153, 2016.

[6] J. J. P. C., Rodrigues, S.S. Compte, I. De la Torre Diez, 'Health Level 7. In e-Health Systems', Theory and Technical Applications, pp. 21–31, 2016.

[7] A. Yachir, B. Djamaa, A. Mecheti, Y. Amirat and M. Aissani, 'A comprehensive semantic model for smart object description and request resolution in the internet of things', *Procedia Computer Science*, 83, pp. 147–154, 2016.

[8] P. P. Jayaraman, A. Yavari, D. Georgakopoulos, A. Morshed, A. Zaslavsky, 'Internet of Things Platform for Smart Farming: Experiences and Lessons Learnt'. *Sensors*, *16*, 1884, 2016.

[9] P. Desai, A. Sheth, and P. Anantharam, 'Semantic gateway as a service architecture for IoT interoperability,' arXiv preprint arXiv:1410.4977, 2014.

[10] S. Jabbar, F. Ullah, S. Khalid, M. Khan, K. Han, 'Semantic interoperability in heterogeneous IoT infrastructure for healthcare', *Wirel. Commun. Mob. Comput.*, 10, 2017.

[11] A. Gyrard, P. Patel, A. P. Sheth, & M. Serrano, 'Building the Web of Knowledge with Smart IoT Applications', IEEE Intelligent Systems, 31(5), pp. 83–88, 2016.
[12] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, 'Role of middleware for internet of things', International Journal of Computer Science and Engineering Survey, vol. 2, pp. 94–105, 2011. [Online]. Available: http://airccse.org/journal/ijcses/papers/0811cses07.pdf.
[13] S. Alam, M. M. R. Chowdhury, and J. Noll, Interoperability of security enabled Internet of things, Wireless Pers. Commun., vol. 61, pp. 567–586, 2011.
[14] A. Galopin, J. Bouaud, S. Pereira, B. Seroussi, 'An ontology-based clinical decision support system for the management of patients with multiple chronic disorders', *MEDINFO 2015: eHealth-enabled Health, pp.* 275–279, 2015.
[15] P. C. Sherimon, R. Krishnan, 'Ontodiabetic: An ontology-based clinical decision support system for diabetic patients', *Arabian Journal for Science and Engineering* 41, pp. 1145–1160, 2016.
[16] Y. V. Zavyalova, D. G. Korzun, A. Y. Meigal, A. V. Borodin, 'Towards the development of smart spaces-based socio-cyber-medicine systems', Int. J. Embed. Real Time Commun. Syst. 8, pp. 45–63, 2017.
[17] G. Li. C. Zhang, Y. Zhang, C. Xing, J. Yang, 'SemanMedical: A kind of semantic medical monitoring system model based on the IoT sensors'. In Proceedings of the 2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom), Chengdu, China, 9 November 2012.
[18] E. Sezer, O. Bursa, O. Can, M. O. Unalir, 'Semantic Web Technogies for IoT-Based Health Care Information Systems', SEMAPRO 2016 : The Tenth International Conference on Advances in Semantic Processing, IARIA, ISBN: 978-1-61208-507-4, 2016**.**
[19] M. Karabatak and M. C. Ince, 'An expert system for detection of breast cancer based on association rules and neural network', Expert Systems with Applications, vol. 36, no. 2, pp. 3465–3469, 2009.
[20] A. S. Nocedal, J. K. Gerrikagoitia, and I. Huerga, 'Supporting clinical processes with semantic web technologies: a case in breast cancer treatment', International Journal of Metadata, Semantics and Ontologies, vol. 5, no. 4, pp. 309–320, 2010.
[21] J. M. Blum, G. H. Kruger, K. L. Sanders, J. Gutierrez, and A. L. Rosenberg, 'Specificity improvement for network distributed physiologic alarms based on a simple deterministic reactive intelligent agent

in the critical care environment,' *Journal of Clinical Monitoring and Computing*, vol. 23, no. 1, pp. 21–30, 2009.

[22] K. A. Kumar, Y. Singh, and S. Sanyal, 'Hybrid approach using case-based reasoning and rule-based reasoning for domain independent clinical decision support in ICU', Expert Systems with Applications, vol. 36, no. 1, pp. 65–71, 2009.

[23] R. C. Chen, Y.-H. Huang, C.-T. Bau, and S.-M. Chen, 'A recommendation system based on domain ontology and SWRL for anti-diabetic drugs selection', Expert Systems with Applications, vol. 39, no. 4, pp. 3995–4006, 2012.

[24] P. Barnaghi, P. Cousin, P. Malò, M. Serrano, and C. Viho. 'Simpler iot word (s) of tomorrow, more interoperability challenges to cope today'. River publishers series in communications, page 277, 2013.

[25] S. Mishra, S. Malik, N. K. Jain, S. Jain . 'A realist framework for ontologies and the semantic Web', *Procedia Comput Sci.*, 70, pp. 483–490, 2015.

[26] S. Mishra, S. Jain, 'Ontologies as Semantic Model in IoT', International Journal of Computers and Applications, vol. 40: 2018.

[27] S. Mishra, S. Jain, 'A Unified Approach for OWL Ontologies', International Journal of Computer Science and Information Security (IJCSIS), vol 4:11, pp. 747–754, ISSN: 1947–5500, 2016.

[28] T. Shah, F. Rabhi, P. Ray, K. Taylor, 'Enhancing automated decision support across medical and oral health domains with semantic web technologies'. In: Proceedings of the 24th Australasian Conference on Information Systems (ACIS) (2013). http://mo.bf.rmit.edu.au/acis2013/382.pdf. Accessed 23 Jan 2014.

[29] Z. Wu, Y. Xu, Y. Yang, C. Zhang, X. Zhu, Y. Ji, 'Towards a Semantic Web of Things: A Hybrid Semantic Annotation', Extraction, and Reasoning Framework for Cyber-Physical System. *Sensors*, *17*, 403, 2017.

[30] A. Rhayem, M. B. A. Mhiri, M. B. Salah, and F. Gargouri, 'Ontology-based system for patient monitoring with connected objects,' Procedia Computer Science, vol. 112, pp. 683–692, 2017.

[31] B. A. Mozzaquatro, C. Agostinho, D. Goncalves, J. M., Ricardo J. G., An Ontology-Based Cybersecurity Framework for the Internet of Things, Sensors, 18, pp. 3053, 2018.

Biographies

Sanju Mishra Tiwari is a Post Doctoral Researcher of Ontology Engineering Group, Universidad Polytecnica De Madrid, Spain. She has worked as a Research Associate for a sponsored research project "Intelligent Real time Situation Awareness and Decision Support System for Indian Defence" funded by DRDO in Department of Computer Applications, National Institute of Technology, Kurukshetra. Her current research interests include Knowledge Based Systems, Intelligent Decision Support, Semantic/Intelligent Query Search Engines, Ontology Integration, Linked Data Generation. She has to-date published 21 research papers two book chapters with international and national publishers. She has worked as a Guest Editor for IGI-Global and Inderscience Journals. She is the member of IEEE. She is working as an organizing committee member for the Conferences and Workshops of MIR Labs, USA. She is a PC Member of Research and Innovation Track in SEMANTiCS 2019 Karlsruhe conference.

Sarika Jain graduated from Jawaharlal Nehru University (India) in 2001. Her doctorate is in the field of Knowledge Representation in Artificial Intelligence which was awarded in 2011. She has served in the field of education for over 18 years and is currently in service at the National Institute of Technology, Kurukshetra. Her research interests are in the area of Intelligent Systems, Ontological Engineering, Semantic Web Technologies, and Linked Open Data

Cloud with an aim to make people understand the importance of semantic web over the traditional web. Dr. Sarika is currently working toward solving the interoperability problem generated by IoT, Big Data and Cloud Computing initiatives. She has authored over 82 publications and five text books including "Information System" and "Mobile Computing". Dr. Sarika has just completed a research project sponsored by DRDO, India worth Rs 40 lakhs. She has constantly been supervising DAAD interns from different universities of Germany and many interns from India every summer. She is a member of IEEE and ACM and a Life Member of Computer Society of India.

Ajith Abraham is the Director of Machine Intelligence Research Labs (MIR Labs), a Not-for-Profit Scientific Network for Innovation and Research Excellence connecting Industry and Academia. As an Investigator/Co-Investigator, he has won research grants worth over 100+ Million US$. Dr. Abraham works in a multi-disciplinary environment and has authored/coauthored more than 1,300+ research publications out of which there are 100+ books covering various aspects of Computer Science. Some of his books/articles were translated to Japanese, Russian and Chinese. About 1000+ publications are indexed by Scopus and over 800 are indexed by Thomson ISI. He has 700+ co-authors originating from 40+ countries. Dr. Abraham has more than 32,000+ academic citations (h-index of 83). He has given more than 100 plenary lectures and conference tutorials (in 20+ countries). Dr. Abraham is the Chair of IEEE Systems Man and Cybernetics Society Technical Committee on Soft Computing and served as a Distinguished Lecturer of IEEE Computer Society in Europe. Currently he is the editor-in-chief of Engineering Applications of Artificial Intelligence and serves/served the editorial board of over 15 International Journals indexed by Thomson ISI. Dr. Abraham received Ph.D. degree in Computer Science from Monash University, Melbourne, Australia (2001).

Smita Shandilya (Senior Member-IEEE) is an eminent scholar and energetic researcher with excellent teaching and research skills. She achieved excellent result in all the subjects she has taught till date. She has over 20 quality research papers in international & national journals & conferences to her credits. She has delivered several invited talks in national seminars of high repute. Her research interests are Power System Planning and Smart Micro Grids. She is one of the core members of the research and development section of her Institute. She is also involved in various projects like the establishment of Energy Lab in the Institute (first in any Private Institute in M.P.), Establishment of Training cum Incubator center in Collaboration with iEnergy.