I.J. Wireless and Microwave Technologies, **2021, 1, 28-46**
Published Online February 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.01.04

An Ontology based Approach for Context-Aware Security in the Internet of Things (IoT)

Asifa Nazir, Sahil Sholla, Adil Bashir
Department of Computer Science &Engineering
Islamic University of Science &Technology, Awantipora, India
Email: {malikasifa356[1], sahilsholla[2], adilbashir.445[3]}@gmail.com

Received: 01 September 2020; Revised: 13 October 2020; Accepted: 03 November 2020; Published: 08 February 2021

Abstract: Due to increased number of IoT devices, the marketplace is showing significant growth of sensor deployments around the world. The context involved in any IoT environment needs proper storage, processing and interpretation to get deeper insights from it. Previous research has not focussed much on context-ware security in IoT environment and has primarily relied on context-ware computing methods. In this research paper we implement logical decisions among IoT nodes in healthcare system using ontological approach. With the help of ontological method collected data is transferred between various healthcare devices to the knowledge base thereby achieving security of context like patient data by providing deeper insights, so as to generate intelligent suggested solutions. Incorporation of context-aware rules based on common experience for specific healthcare scenario is done to get implicit insight among IoT nodes. This work designs security ontology using Security Toolbox: Attacks & Countermeasures (STAC) framework that is implemented in Protégé 5. Moreover, Pellet (Incremental) reasoned is used to evaluate the ontology. Emergency ontology that can prove helpful at emergency times has also been designed. Different parameters addressed in this work are authentication, access-control, authorization and privacy using context-awareness methodology that can enable naive users make informed security decision.

Index Terms: IoT, semantic web, attacks, counter-measures, context-aware security

1. Introduction

Internet of Things (IoT) is the concept of pervasive interconnected computing things, services and humans each provided with unique identifiers to achieve common goal of data transmission in smart applications without requiring human intervention. IoT has become particularly popular because of the speedy development of small sized and low cost sensor devices in market. Typical applications of IoT practices include smart home, smart healthcare monitoring systems, smart agriculture system etc. IoT aims to create an environment where various things flawlessly interact with each other to provide advanced smart services for humans. The interconnected devices such as sensors at perception layer of IoT monitor and hence collect data from particular environment and then after in-depth analysis of the data useful information is extracted to enable promising smart civic amenities available at application layer [1].IoT framework helps services, device and humans to communicate using existing communication technologies (like Bluetooth, Zigbee etc.). According to experts the estimated amount of IoT devices in world is exceeding world's population [2]. In 2017, it has been estimated that the number of connected IoT devices in world is about 8.4 billion and is expected to grow in future. According to predictions made by Cisco's, the number of devices associated to the internet will be more than 50 million by 2020[3]. Movement of the data in context-aware system is determined by context-aware life cycle comprising of four phases. The first phase called context acquisition is accountable for data collection from various physical or virtual sources. The second phase known by the name of context modeling is responsible for modeling data in well-defined manner. This modeled data is processed further to derive high-level situational information from low-level situational information which is done in third phase called reasoning phase. Lastly, distribution of high as well as low–level context is done in fourth phase known as dissemination/distribution phase [4].

Context-awareness is the process of analyzing the changing behavior of surroundings in which IoT devices are to be deployed. This term was first introduced by Schilit and Theimer in 1994, later redefined by Ryan et al. [5, 6]. In both cases main emphasis is on computer applications. Abowd et al. stated that these definitions are too specific and can't be used to specify whether a given system is situation-aware or not. The more appropriate definition of context-awareness is as follows:

"A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task [7]".

Due to the presence of increased number of advanced sensing technologies in market large number of sensor devices with smaller size, cheaper cost and good in strength huge amount of data is generated continuously. Without analysing this huge amount of data generated from sensors, it becomes significant to gain some valuable information. To deal with this challenge context-aware computing engages an important role. Context-aware computing enables us to store contextual information associated to sensing devices thereby interpreting the context in an easy and meaningful way. Understanding context in an easy way means that machine–machine communication is at ease being the fundamental part of IoT. In order to continuously control the process of interaction between various devices and implement logical decisions with dynamic adaption to contextual situations in smart environment, context-awareness has a major role to play. For example, continuous context-awareness monitoring is essential in case person is admitted to hospital so as to adapt dynamic changes of patient's condition. Before discussing about context-aware systems let us define the context first. Due to lack of consensus with respect to meaning of context, several definitions can be found in literature: Context has been defined as location, identities of surrounding people, devices and modifications to these devices with time [5, 6]. In the beginning of context-aware systems such definitions were used with respect to context in literature but with time other definitions were also given. Context can also be defined as an emotional state of a person, current emphasis, present position, direction, surrounding devices or people, date and time [8]. Other common ways of defining context was simply practice of synonyms. Some authors defined context as the characteristics of current situations. Above definitions are too wide, a better one has been provided by Brown. Brown defined context as fundamentals of user's environment which the computer recognizes about [9]. More accurate definition was presented by Dey and Abowd as follows:

"Any information that can be used to characterize the situation of entities (i.e., whether a person, place or object) that are considered relevant to the interaction between a user and an application, including the user and the application themselves" [10].

Some author's classified context based on the difference between context dimensions called as external and internal [10].Context has also been classified as physical context and logical context [11].The external or physical dimension is the context that can be investigated by hardware devices like location, light, sound, movement, temperature, pressure while as the internal or logical dimension is one specified by user interactions like user's emotional state, working context, objectives etc. Context can be distinguished on the basis of three entities: place (buildings, rooms etc.), person (individual, class of people etc.) and thing (hardware devices like sensors etc.). All these entities can be better described by characteristics such as identity, location, status and time [10].

Context awareness models must support context data acquisition, representation, storage and reasoning within an application [12].Henricksen defined context model and context attributes in much more appropriate way as follows:

"A context model identifies a concrete subset of the context that is realistically attainable from sensors, applications and users and able to be exploited in the execution of the task. The context model that is employed by a given context-aware application is usually explicitly specified by the application developer, but may evolve over time [13]."

"A context attribute is an element of the context model describing the context. A context attribute has an identifier, a type and a value, and optionally a collection of properties describing specific characteristics"[13].

Context models define and accumulate data so as to recognize existing subsections of context obtained from sensors, applications and users with good ability of being exploited while executing a particular task. The process of developing flexible and useful context ontologies covering wide range of contexts is very challenging task. Various models present in literature are: *Key-Value models*, *Markup scheme models*, *Graphical models*, *Object oriented models*, *Logic based models*, *Ontology based models*. A summary of different context modelling ontology techniques, based on data structure which can be used to represent and exchange contextual information in particular system is presented in [14].

Ontologies are the most communicative and user-friendly models fulfilling most of the user requests. In order to design better context ontology various requirements are simplicity, flexibility, genericity and expressiveness [15].Therefore, formal depiction of the facts is done by a set of notions within a particular area and the associations between those concepts. Ontologies are very auspicious tools used for modelling contextual information because of their extraordinary expressiveness with greater opportunity of applying ontology based reasoning methods, facility of interoperability among devices which would not otherwise actually work together. Ontologies are the basic requirements for structuring a particular context-aware system where autonomously developed sensors, devices and various kinds of facts share knowledge in open and dynamic distributed systems thereby providing pertinent amenities and information to users based on present context [4].

Many components involved in ontologies are individuals, attributes, concepts, relationships etc. Moreover, ontologies are mainly developed in two stages .At initial stage the area and hence various choices available must be clearly known. In second stage review must be made related to existing ontologies already available so as to find the limitations present in them [16, 17]. The semantic specifications of different sensors are presented in paper [18]. Many tools are accessible to define, present and share ontologies developed by the World Wide Web Consortium. To develop more dynamically adaptive user friendly systems, addition of various parameters like light, noise or location allows evolution of high-level context-aware systems [4].

Security is a chief concern in all context-aware computing systems whether smart healthcare or smart home as in IoT ,data needs to be collected at the lowest level and this collected data (location, medical data, particular plan of military officials etc.) may contain sensitive confidential information that must not be disclosed to anyone without proper authentication mechanism. Therefore, extreme care is must while collecting, modelling, reasoning, storing or distributing data. Enforcement of secure communication protocols at each IoT layer is significant, scrutinizing and controlling the access with context-aware rules. For this reason context toolkits were included with the concept of context ownership providing features for dynamic adaptation of access rules defined for particular application. For instance, if a patient is allergic to certain medical treatments it must be quickly made available to doctor and nobody else even if patient does not give direct sign. From this it is clear that context-aware security must to be applied automatically with inherit sensitivity rules defined. Moreover, system must be able to avoid malicious users to exploit sensitive information of patient. In this paper, we present an ontology based context-aware security solution to healthcare system.

Because of the increased number of advanced sensing devices in the IoT world with smaller size, cheaper cost and better battery capacity, huge amount of data (context) is generated. This huge amount of data needs to be processed and analysed to get some valuable information. To deal with this challenge context-awareness has an important role to play. Context-aware computing allows us to store context associated to sensing devices at perception layer of IoT and hence analysing the context using context collection, context modelling, context reasoning and context distribution. Different context models: Key-Value models, Mark-up scheme models, Graphical models, Object oriented models, Logic based models and Ontology based models are present in literature which can be used to define and accumulate context obtained from sensors or applications. In this study we are using ontological approach to achieve our objective. The reason we have chosen this approach is because of its communicative, user-friendly and extraordinary expressiveness facilitating interoperability among devices. Our chief concern is to provide security in smart healthcare environment. Security being the chief concern in all context-aware systems whether smart home, smart agriculture or smart healthcare where context is to be collected at lowest level containing confidential data. Therefore, enforcement of secure communication between IoT nodes becomes significant with introduction of context-aware rules specific to smart healthcare. This paper seeks to achieve security in healthcare environment in dynamical way with the enforcement of context-aware security rules specific to the context available. Many researchers have contributed in the field of IoT by providing context-awareness architectures, however security aspects merit further research. This work seeks to achieve context-aware perspective of security that will allow automatic adaption of the behaviour according to context. This paper uses ontological approach to provide situation-aware security in healthcare domain. Using the process of ontology approach data collected using various sensors at perception layer of IoT is transferred among different healthcare devices. This data is then transferred to the knowledge base to achieve deeper insights thereby achieving security of context such as patient data and generate intelligent suggested solutions. The rest of this paper is organized as follows: Section 2 presents a related work on context-aware security systems in various domains of IoT. Section 3 describes in detail STAC (Security Toolbox: Attacks and Countermeasures) as a technology. In Section 4 we present our proposed approach in detail throwing light on various context-aware rules and semantic languages used in this paper. In Section 5 a generalized framework for context-aware security is provided. Section 6 shows evaluation and implementation of our use-case scenario using protégé. Finally, paper is concluded in Section 7.

2. Related Work

Context-awareness is process of discovering the contextual situations using particular context awareness model to provide corresponding solution based on the awareness analysis. Context-aware computing is movable computing standard where applications can realize contextual information like location, time etc. and adapt to situations accordingly. Number of projects representing majority of research in context-aware computing with proposed solution sets based on the evaluation and analysis highlighting various lessons learned from their study with possible future directions have been presented in comprehensive manner in [4].

ArbiaRiahiSfar et al. have given a road map to various challenges in IoT paradigm. The challenges in IoT mostly result from intrinsic security vulnerabilities of IoT devices while interacting with other devices in smart environment. They surveyed various security related issues and counter-measures present in literature. They concluded that because of the involvement of more IoT devices in environment day by day security issues increase. Therefore, self-sufficiency of IoT objects perceiving contextual situations and activating required actions can help devices to operate accordingly [19]. According to the survey major security issues in IoT result from intrinsic security vulnerabilities of IoT nodes and

hence need of self-sufficiency of IoT devices is must.

Laplante et al. presented a well-organized strategy for explaining smart healthcare by providing a comprehensive overview of various security requirements inside [20]. Herzog et al. presented an openly accessible OWL based ontology of information security modelling assets, threats, vulnerabilities and countermeasures and their associations. The ontology presented can be used as a wide-ranging vocabulary in the area of information security. The presented ontology is useful in understanding reasoning between various entities involved such as threats and countermeasures. This paper explains the presented ontology with its application, possible extensions, implementation and tools to work with it [21]. This paper presented an openly accessible OWL based ontology focussing on threats and corresponding counter-measures at each IoT layer. Savola et al. in their paper have presented various security concerns to be considered for medical systems including scrutiny of risk-driven security metrics for elderly and disable people from the viewpoint of end-users and service-providers. In this paper they have recognized the key risks and their influence along with a list of security concerns for each risk [22].However, their work focussed on restricted number of use-cases like patient monitoring without scaling to wider use cases like medication management systems etc.

Mozzaquatro et al. presented a paper focussing on the enhancement of IoTcybersecurity. Using an ontological approach they recommended suitable security services that must be adopted to address specific threats [23].Gonzalez-Gil et al. presented the data security ontology for IoT (DS4IoT) by following ontological evaluative processing using novel semantic concepts. The presented work is justified by mapping the DS4IoT ontology to the NGSI-LD data model [24].The security ontology presented in their paper may act as reference ontology for naïve researchers with predefined semantic terms. However, description of context-aware rules is not described in clear manner. Ayele et al. proposed, developed and evaluated IoT security ontology for smart home energy management system (SHEMS) in smart grids. In this research they extended the SAREF energy management ontology with satisfactory security features and checked their efficiency by running SWRL rules and SPARQL queries [25].Implementation of rules and their evaluation is done in proper manner.

Many security guidelines were issued by different organizations for health care devices like FDA published a guide named as *Postmarket Managementof Cybersecurity in Medical Devices* [26]. Likewise, risk assessment questionnaires for the use of medical equipment in U.S military were provided by the Naval Medical Logistics Command (NMLC) [27].However, these efforts mainly consider medical equipment manufacturers and do not take other participants like medical professional into account. Moreover, they have provided generalized security suggestions focussing on one part of smart healthcare environments to the omission of other-end such as back-end.

An ontology of security requirements for web applications, describing concepts of stakeholders, assets, vulnerabilities and threats is presented in [28].The main aim of this research is to enable the reuse of knowledge about security requirements while developing various web applications. SecWAO presented by Buch and Wirsing with the aim to provide security on a secure web application provisioning web developers with security requirements to design better ontologies [29].This paper can prove useful for web applications defining security requirements in mannered way.

Parkin et al. presented an ontology describing best security practices based on ISO 27002 standard showing the effect of human behaviour on securing information in terms of insights and suggestions[30]. This security ontology can help security managers to make intelligent decisions in an organisation. Tao et al. presented an ontology based security provision architecture supporting security and privacy by defining a sharable security vocabulary used by facility providers, customers and semantic web reasoner[31].The presented ontology has provided a generalized vocabulary which can help naïve users to identify their security requirements specific to the context available.

IoT Security Ontology(IoTSec) were presented by B. A. Mozzaquatro et al. representing information about security in the form of assets, threats and security mechanisms using expressive semantics [32]. SecAOnto an ontology validating knowledge on security assessment by concentrating on various security aspects addressing relationship between information security and software assessment build onto the top of STAC [33]. In our paper we propose context-aware security for smart healthcare system using ontological approach. An ontological based approach identifies a list of scenario-specific security related issues therby recommending possible counter-measures.

3. STAC as a Technology

STAC is a security ontology that has been developed with features for non-security experts or software developers to help them in recognizing and be cognizant of main security concepts like attacks, security properties, security assets or countermeasures and hence design secure software's. The basic feature of STAC is its simplicity to identify relationship among different security concepts in the given contextual system. It is a graphical database which can used to provide intelligent solutions by inferring the relationship between the contexts discovered. This ontology data model can prove useful if applied to a set of individual facts thereby creating a knowledge graph by inferring relation among nodes of different type. The M3 (machine to machine measurements) approach has inspired the STAC approach by addressing various questions as follows:

1. How to provide assistance to developers using a 'security by design' approach, in securing IoT applications?
2. How to secure IoT architectures and applications servicing various technologies?
3. How to make use of existing security ontologies for security purpose?
4. How to deliver a cross-domain security knowledge base?
5. How to provide a knowledge base following the best practices of semantic web?

STAC is a security ontology that has been developed for non-security experts, software developers to help them in recognizing and be cognisant of main security concepts like attacks, security properties, security assets or countermeasures and hence design secure software's. The main purpose of this ontology is to recommend and hence suggest best security mechanisms to protect particular application. To accomplish this goal STAC ontology specifies the relationship between several concepts such as attacks, security mechanisms, technology, security property, OSI model and features. In STAC ontology attacks are classified according to the OSI model layer specific to technology. For example, SQL injection occurs at application layer targeting web application and jamming attack that occurs at physical layer specific to sensor network technology. We in this paper took help from STAC ontology and created our use-case scenario using Protégé. The STAC ontology identifies the associations between main security concepts such as cryptographic concepts, security tools and security protocols therby classifying security attacks at OSI layer with corresponding security mechanism. The application users or developers use STAC security knowledge base to identify attacks with corresponding countermeasures precise to the technology used in particular application. The various components of STAC ontology that participate to provide context-aware security in any IoT domain are: STAC template generator, STAC nomenclature, STAC interoperable domain knowledge and LOV4IoT [28].

STAC template generator finds attacks and security measures corresponding to the technologies used in particular application. The STAC nomenclature uses common terms with the aim to avoid ambiguities. For example a beginner in security may not know that symmetric algorithm is a synonym for public key algorithm. To avoid such ambiguities common terms are used to ease interoperability between already existing works. In LOV4IoT dataset security ontologies have been classified with reused option to build the interoperable knowledge base. To reuse security knowledge with LOV4IoT more than 24 ontology-based workings in the LOVIoT dataset related to different technologies were explored and classified by [29]. Because of their numerous limitations like issues regarding the security proficiency such as lack of semantic web best practices, non-sharable nature of ontologies online, use of heterogeneous relationships etc. Gyrard et al. restructured an interoperable security knowledge base called STAC (Security Toolbox: Attacks & countermeasures) with the ability to link various security fields together [30].

4. Proposed Approach

Healthcare is a substantial field comprised of huge knowledge base originating from various medical diagnostic devices. The type of context in healthcare may be patient data, status of system admin or the data related to medical professionals. Authorities in healthcare are required to manage huge amount of data determining important healthcare decisions. However, due to heterogeneity and complex nature of data generated; it becomes necessary to provide adequate security to sensitive data of various stakeholders in healthcare system. Number of security challenges may overstrain fundamental capabilities of rationality and reasoning of highly proficient expert's thereby putting the lives of patients in danger. This paper tries to epitomise and hence exchange the context of various types in healthcare environment in secure fashion. In this paper we provide a conceptual overview of how to provide context-aware security in healthcare environment for patient type of context exchanged between devices. We have used semantic approach to allow sharing of context in IoT therby achieving context-aware security.

The main aim of this research is to provide context-aware security of data with regards to patient context such as treatment history, test description, current location or cause of the disease. We have constructed a security ontology using the concept of STAC (Security Toolbox:Attacks and Countermeasures) security ontology. Security and privacy are the major concerns in IoT environment. Long back people prefer security mechanisms that use non-aware approach in which static parameters were used to provide security. Security mechanisms un-aware with context can be inefficient for IoT due to its dynamicity and heterogeneous nature. Thus, context-aware security is the feasible option to provide security in dynamic IoT environment. By using contextual information of IoT in changing environment, dynamic security is provided. The information in context can be used to reconfigure security mechanisms and adjust required security parameters according to the need of situation. In this paper we use semantic approach that allows sharing of context in IoTtherby achieving context-aware security. The parameters we address in this paper are authentication, authorization, access control and privacy.

Traditional authentication mechanisms demand much user interactions such as manual logins, logouts etc. Because of their context-insensitive nature they were not able to adapt security permissions with changing context. Consistent authentication mechanism is the basic requirement in IoT with its changing context for secure systems. The technologies we can use to provide proper authentication mechanisms are face recognition, biometric or iris scanner.

Authorization and access control although different but we try to reach both of them together. Many security systems already present assure their security with permit (allow) and rebuff (deny) based strategies where permit means

granting access to requester and rebuff means blocking access from requester when credentials don't match. Such type of security systems consider only static parameters and are less secure to be used in IoT environment. For IoT environment we need to consider the contextual information to enforce better security policies that can potentially enhance the effectiveness of security decisions.

Privacy is the main concern in any security system that must be addressed precisely so as to ensure information is private. Information's like travel routes, buying habits and other daily activities that must not be disclosed. Better privacy preservation can be achieved by considering full context information into account.

The use of semantic approach facilitates heterogeneous computing devices in IoT to have shared set of concepts related to context when interacting with each other. Ontological engineering allows re-use of context of well-known domains in IoT without initiating from the scratch. Because of context sharing via ontological engineering, the processing effort of various entities is reduced. Let's consider a situation to show the advantage of using semantic approach of context sharing. In this scenario, the emphasis is on sharing the context of an employee in office when some emergency occurs. The context information is collected by sensors connected in office's dispensary room therby prompting the event of the employee having heart attack. This event must be shared with systems of interest such as ambulance may receive information about event to attend patient. The received context information can further be used in other required processing's like this information can be shared with urban traffic infrastructure to channel the traffic with a "green wave" in traffic lights so as to reduce waiting time of patient in ambulance. This work provides security among various IoT nodes using Protégé ontology toolkit. A clear-cut conceptual overview of various security requirements, expected counter-measure and other related concepts with regards to healthcare system are provided. We have successfully generated our security ontology based on common security requirements using protégé. The difference with this proposed approach with traditional approaches is that it uses dynamic /context-aware approach providing efficient security in heterogeneous environment. Furthermore, the language we have used to construct our ontology is OWL thereby incorporating context-aware rules based on common experiences in healthcare environment. With the process of sharing context among devices using semantic approach, feature of context-awareness is achieved between them. With this sharable context the reconfiguration and readjustment of context (security requirements) is done according to the need. The security parameters addressed in this study are authentication, authorization, access control and privacy. Using OWL we have described the structure of our healthcare system in terms of classes, instances, relations, data type properties and object properties. Moreover, a healthcare ontology for effective handling of context during emergency situations is also constructed. The tools we can use for implementation and evaluation of our ontology efficiently are Protégé, Oops (ontology pitfall scanner), RDF validator, Triple checker etc. In this paper we use Protégé 5.5 to develop our security ontology for healthcare system. Moreover, we developed a healthcare ontology for effective handling of context during emergency situations shown in Fig.9.

4.1Context-aware rules

Context-aware security rules are semantic rules or SWRL (Semantic web rule language) represented as implication between antecedent (body) and consequent (head) applicable on OWL ontologies enabling reasoner to make inferences and deductions based on present scenario. In this work the rules are specific to healthcare system and are determined based on the contextual situations that may arise in healthcare environment. These rules are relevant to this research because they identify relationship among different IoT nodes thereby inferring relations that are implicit. We can add more rules based upon our common experience from healthcare system. The intended meaning can be read as whenever the conditions specified in the antecedent hold then the conditions specified in the consequent must also satisfy. Application of rules whether context-aware rules to diagnose health condition of patients or context-aware security rules providing security with regards to patients data enriches information in more appropriate way by providing logical relationship between involved entities. In our case contextual use-case scenario is given as input to Protégé tool thereby incorporating context-aware security rules to output and identify security issues in the scenario if any, and recommending suitable security mechanisms. As SWRL rule consist of an antecedent and consequent which internally comprise of positive conjunction of zero or more atoms. Further, SWRL does not support negated atoms or disjunction. An antecedent with zero atoms inside is considered trivially true (satisfied by every interpretation) implying that consequent must also be satisfied by any interpretation [34]. A consequent which is empty inside is trivially treated as false means it is not satisfied by any interpretation. An antecedent or consequent with multiple atoms is taken as a conjunction of different atoms. The generalized structure of SWRL is as follows:

atom^atom^atom…..->atom^atom^atom…

Atoms in SWRL rule can be of the form A(x), where A is an OWL description and x is variable. An OWL description can be class atom, object valued property atoms or data valued property atoms. For example, class atoms can be patient(?p), object valued property atom can be hasSecurityMechanism(?sm) and data valued property atom can be hasAge(?p,?age). In order to define SWRL there are various syntax forms like abstract syntax (functional form), XML concrete syntax or human-readable form (involving logic predicates). In our project we use human-readable syntax to express and infer our information in the form of rules. Each rule is expressed with the help of conjunction

operator expressing relationship between various atoms involved and each prefixed with ?mark. A simple example defining SWRL rule using human-readable syntax is given as follows:

$$\text{hasSecurityMechanism}(?x_1,?x_2)\text{^}\text{SatisfiesSecurityProperty}(?x_2,?x_3) \rightarrow \text{SecurityAssetSatisfiedBy}(?x_1,?x_3)$$

The above rule is interpreted as "x_1" is having security mechanism "x_2" and security mechanism"x_2" is satisfied by security property "x_3". According to the information given in antecedent, an inference that can be drawn on consequent side is that security asset "x_1" is satisfied by security property "x_3".This is how semantic rules work while incorporating them with the present use-case scenario and hence inference of new knowledge from given information.Table1 shows XML syntax of above rule. In protégé we have rule tab to do such operation and can add rules of our need accordingly. There are actually three steps that go hand in hand to infer knowledge from information present on antecedent side. These are: OWL+ rule transferred to Drools engine, Running Drools and finally statements inferred back to OWL reasoner. In protégé we list our rules of interest at the top-most part of rule tab and at the bottom-most part various control tabs can be used to control their execution. Drool engine is a tool that is able to apply the rules we write. Firstly we incorporate rules with our security ontology and feed them to the "Drools engine". The second step is actually running of these rules using "run Drools tab". After running our rules we can see all the consequences of running those rules which can be inspected using "inferred axioms tab" and finally in the last step we can add the inferred results back to our ontology using "Drool->OWL tab".

Table 1.SWRL implication

```
<ruleml:imp>
<ruleml:_rlabruleml:href="#source">
<owl x:Documentation> The Security Expression</owl x:Documentation>
<ruleml:_body>
<swrl x:IndividualPropertyAtomswrl x:Property ="Security :hasSecurityMechanism">
<ruleml:var>x1</ruleml:var>
<ruleml:var>x2</ruleml:var>
</swrl x:IndividualPropertyAtomswrl x:Property="Security:Satisfies">
<ruleml:var>x2</ruleml:var>
<ruleml:var>x3</ruleml:var>
</swrl x:IndividualPropertyAtom>
</ruleml:_body>
<ruleml:_head>
<swrl x:IndividualPropertyAtom swrl x:property="Security:SecurityAssetSatisfiedBy">
<ruleml:var>x1</ruleml:var>
<ruleml:var>x3</ruleml:var>
</swrl x:IndividualPropertyAtom>
</ruleml:_head>
</ruleml:imp>
```

The inference rules given above are means which permit novel facts to be determined from indirect information. The rule above has found a new relationship when a set of axioms satisfied the requirements of rule. For better understanding of inference mechanism, we show graphical representation of this inference rule as follows:

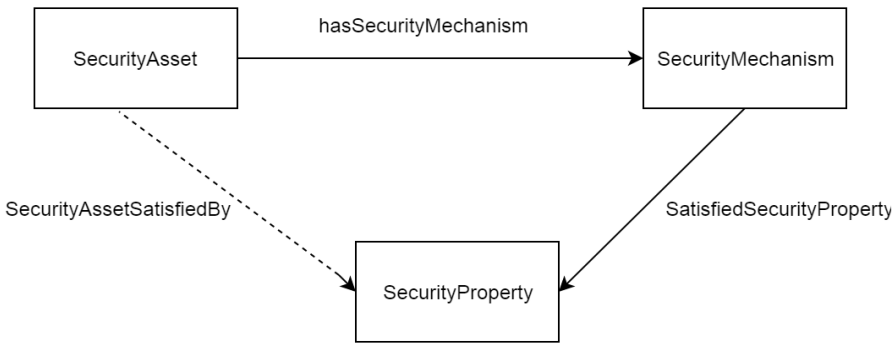

Fig.1.Rule inference

In the above Fig.1 object property hasSecurityMechanism(?x_1,?x_2) establishes a link between security asset "x_1" and security mechanism "x_2".Similarly ,object property SatisfiedSecurityProperty establishes link between security mechanism "x_2" and security property "x_3".The inferred knowledge (new fact) is represented in dotted lines with regards

to object property SecurityAssetSatisfiedBy.

The context in IoT is composed of sensitive domains such as healthcare, transportation etc. It is highly significant to protect sensitive information from various security threats. It is even more difficult to manage the context in dynamic environment with number of people continuously joining and leaving that particular area. The fundamental process to provide context-aware security is by using pre-defined context-aware rules within specific domain. Description of various context-aware rules used in this paper is presented below:

The formation of inference rules and hence their establishment is done with the help of SWRL (semantic web rule language) with protégé SWRL tab using semantic reasoner (Pellet, HermiT etc.)[35].The reasoner Pellet operates the ontology logic with the help of inference rules by reasoning with individual, user-defined data type and error correction mechanism for ontologies [36].

Rule1

threatens(?t,?a)^hasSecurityMechanism(?t,?sm)->thwarts(?sm,?a)

This rule shows threat 't' threatens security asset 'a' and has security mechanism 'sm'.The inference generated from this rule is that security mechanism 'sm' prevents threat on security asset 'a'.

Rule2

hasRequirements(?p,?a)^protectsInlayer(?sm,?sp)->satisfies(?sm,?sp)

This rule says context type patient 'p' has security requirements to secure security asset 'a' and security mechanism 'sm' protects security property 'sp' in particular layer. From this rule inference drawn is that security mechanism 'sm' satisfies security property 'sp'.

Rule3

threatens(?t,?sp)^thwarts(?sm,?t)->hasSecurityMechanism(?t,?sm)

As per this rule threat 't' threatens security property 'sp' and security mechanism 'sm' prevents threat 't' which infers that threat 't' has security mechanism 'sm'.

Rule4

hasSecurityMechanism(?a,?sm)^SecurityProperty(?sp)^threatens(?t,?a)^vulnerableTo(?p,?t)^hasSecurityMechanism(?t,?sm)->satisfies(?sm,?sp)

From this rule the object property hasSecurityMechanism(?a,?sm) establishes a link between SecurityMechanism(?t,?sm),threat(?t,?a) and vulnerableTo(?p,?t) therbyinferencing a new relation between threat(?t,?a) and SecurityProperty(?sm,?sp) which is satisfies(?sm,?sp).Fig.2 shows rule incorporation in the present use-case scenario using Protégé. Explanation of each rule defined in the figure is given in well-defined manner rule by rule.

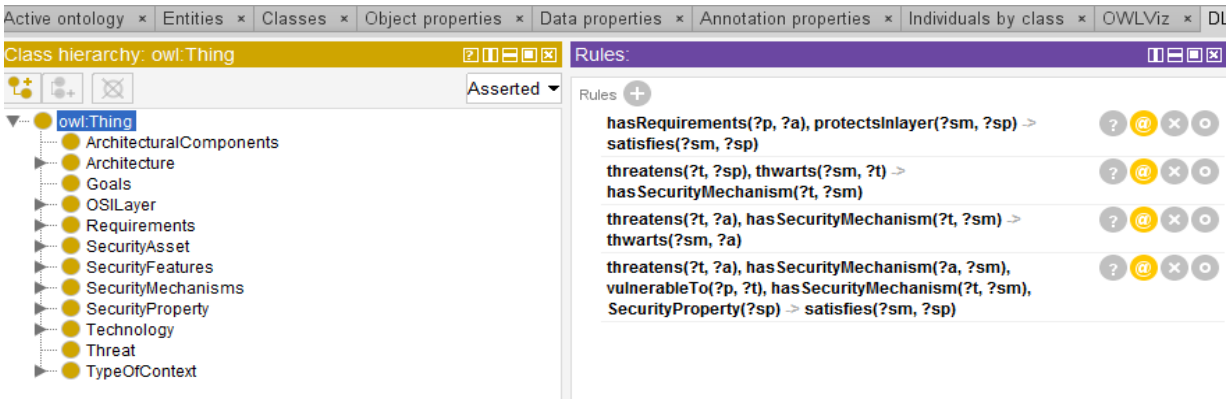

Fig.2. Rule incorporation

Various other diagnostic/context-aware and context-aware security rules are defined with full description of their use.

Rule5

Patient(?p)^hasSymptoms(?p,Throbing_pain_in_one_particular_area_of_head)^hasSymptoms(?p,Na usea& vomiting) ^hasSymptoms(?p,Sensitivity to light)−>doTest (? p, Migraine)

This rule shows that if a person is suffering from intense pain in one particular area of head with the symptoms of nausea, vomiting and sensitivity to light then he/she must go for migraine test.

Rule6

Patient(?p)^hasDisease(?p,Migraine)^hasEvent(?p,Aura)^hasTreatement(?p,AntiflammatoryPainRelievers) −>hasRisk (?p,HeartDisease)

Rule6 determines the consequence of patient suffering from migraine with event Aura treated with antiflammatory pain relievers. The result obtained from above rule shows the patient with such treatment details has risk of heart disease.

Rule7

Patient(?p)^hasEvent(?p,Aura)^hasRisk(?p,HeartDisease)−>hasAlert(?p,HeartDiseaseAlert)^hasMessage(HeartDiseaseAlert,Aspirin_325mg_1tablet_perday)

Rule7 suggests suitable medicine for migraine patient with event of Aura and risk of heart disease.

Rule8

Patient (? p) ^hasEvent (?p, BloodCancer)→has risk (? p, Death)

Rule8 infers that if the patient is suffering from blood cancer then he/she is having risk of death.

Rule9

Patient(?p)^hasSymptoms(?p,Fever)^hasSymptoms(?p,Bonepain)^hasSymptoms(?s,Jointpain) −>doTest (?p, Dengue)

Rule9 verifies the context of patient by determining the symptoms it has. In the above rule patient is suggested to do test for dengue.

Rule10

Patient(?p)^hasDisease(?p,Diabetes)^hasEvent(?p,Hyperglycemia)^hasTreatement(?p,Insulin)−>hasRisk(?p, Aggrevated-Hyperglycemia)^hasEvent(?p,Insufficient-use-of-Insulin)

Rule10 determines the risks and the results of hyperglycemia regarding diabetic patient. In this rule result shows the risk of aggrevated-hyperglycemia and an event detected is insufficient use of insulin.

Rule11

Patient(?p)^hasEvent(?p,Hyperglycemia) −>hasRisk(?p,DiabeticComa)

Rule11 determines the risk of event hyperglycemia. This rule shows that if an event of hyperglycemia occurs then risk of diabetic coma event is possible.

Rule12

Patient(?p)^hasEvent(?p,InsufficientUseOfInsulin)^hasRisk(?p,AggravatedHyperglycemia) −>hasAlert(?p,HyperglycemiaAlert)^hasMessage(HyperglycemiaAlert,Sulfonylureans_500mg_1tablet_perday_in_association_with_Insulin)

Rule12 recommends an adequate treatment for diabetic patient having an inefficient use of insulin in his/her body with the risk of hyperglycemia event notifying patient with suitable medicine alerts.

Rule13

Patient(?p)^HealthDevices(SmartBP)^has Sensors(?p,SmartBp)^BloodPressure(?b) ^diagnose(SmartBP,?b)^hasValue (?t, ?v)^swrlb:greaterThan(?v, 180) →hasEvents(?p, HeartAttack)

Rule13 aims to verify the effect of context when patient is wearing smart healthcare devices to sense blood pressure and hence make decision based on the observed value. This rule verifies that if the blood pressure level (?b) is greater than 180 then patient is attacked by heart attack event.

Rule14

Patient(?p)^hasdetails(?p,TreatementHistory)^hasdetails(?p,TestDescription)^beingPresent(?p,SurgeryRoom) −>hasEvent(?p, surgery)

Rule14 allows the occurrence of event surgery with the process of verified details of patient such as treatment history, test description etc.

Rule15

Patient(?p)^hasPatientdetails(?p)^vulnerableTo(?p,securityAttacks)^Threatens(?p,securityProperty) −>hasRisk(?p,Death)

Rule15 shows that if patient's data is attacked by an adversary via unauthorized access therby threatening security property has risk of death.

Rule16

Patient(?p)^haspatientDetails(?p,treatmentHistory)^hasEmergency(?p,alergicTo)^forwordinformatioTo(?p,doctor)^blockinformationTo(?p,unauthorizedusers)−>hassecurityAgainst(?p,malicioususers)

Rule16 how confidential information regarding patients health during emergency situation must be protected against malicious users by blocking information to unauthorized users and allowing information only to authorized users(doctor, nurse, technical assistant etc.).

Rule17

Patient(?p)^interactsWith(?p,solutionType)^has(?p,securityArchitecture)^vulnerableTo(?p,securityAttacks)^occursInlayer(?p,OSI_layer)^threatens(?p,securityProperty)

−>hasSecuritymeasures(?p,securityMechanisms)

This rule gives generalized view of how attacks are possible in particular solution type architecture occurring in OSI layer with suitable countermeasures.

Rule18

Patient(?p)^interactsWith(?p,wearablesolutionType)^vulnerableTo(?p,authenticationIssue)^threatens(?p,authenticationProperty) −>hasSecuritymeasures(?p,cryptographicTechniques)

In this rule patient interacts with some wearable solution type which may be vulnerable to issue say authentication threatening authentication property can be secured using cryptographic techniques(hash functions, DES etc.)

Rule19

Patient(?p)^hasPatientDetails(?p,treatmentHistory)^vulnerableTo(?p,unauthorizedAccess)

−>protectedBy(?p,biometricAuthenticationmechanism)

In the above rule patient has various details like patient treatment history, test description etc. which may be vulnerable to attacks such as unauthorized access can be protected by providing modern authentication mechanisms (iris scanner, biometric scanner etc.).

4.2 Semantic Languages

The languages that we can be used to represent the interested information semantically are RDF and OWL.RDF is a formal language that is used to describe well-thought-out information, observed as the basic depiction format for developing semantic web. The goal of RDF is to enable application to exchange data on the web while still preserving their original meaning. RDF document describes a directed graph which is actually composed of set of nodes linked by directed edges both of which are labelled with identifiers so as to be distinguished from each other. RDF is a common acronym within the semantic web as it forms one of the fundamental building blocks for forming the web of semantic data. It is basically a graphical type of database used to build the semantic web globally consisting of resources related to each other having any particular inherent importance over other. RDF offers a flexible graph-based model for recording data exchangeable globally that the semantic web uses to store data and RDF is the format in which it is written. RDF can be programmed with semantic metadata using two syntaxes: RDFS and OWL. Both RDF and OWL are W_3C specifications.

RDFS (RDF Schema) is a general purposes representative language recommended by w_3c that defines the semantic vocabularies for RDF resources and defines ontologies by using definitions of vocabularies, taxonomies, properties and relationships between classes. RDF is thus simply a way of data modelling and RDFS is an extension of RDF that provides schema level information [37]. A more detailed way of expressing any ontology is achieved by using OWL(web ontology language) that is semantic extension of RDFS.

OWL is a descriptive logic based language that is built on RDF. In this paper we use OWL to represent our information semantically. RDF can be used to model things of interest using subject-predicate-object statements known as ‘triples’. The prime purpose of building any ontology is to categorize things in terms of semantics [38]. In Table2(a) Class, defines a class called ‘Doctor’ which is subclass of a class named as ‘MedicalProfessional’ which is declared as a disjoint class with class called ‘Patient’. The owl:disjointWith means that the class extension of a class description has no members in common with the class extension of another class description. In owl classification of things is hence done through the use of classes, subclasses and the instance of which are called as individuals. Further, the individuals that are members of given owl class are called class extensions. In Table2(b) shows that individual ‘John’ with patientID ‘P301’ is an instance of RegisteredPatient .

The individuals in owl are linked by two properties named as data type properties (owl:DatatypeProperty) and object type properties (owl:ObjecttypeProperty). The data type properties relate the individual instances of owl classes with the literal value whereas object type properties in owl describes the relationship between individual instances of the owl classes [36]. In above schema Table2(c) defines relationship between an instance ‘Technical Assistant’ of a class to the data value (non-negative in nature) belonging to the range of the XML Schema (http://www.w_3.org/2001 /XML Schema# float) data type via property called “Monthly Salary”. Finally, the Table2(d) in the above example

shows relationship between instances ‘Type of context’ and ‘Security Requirement’ of owl class via property ‘hasRequirements’.Further, the inverse property known as inverseOf defines the same property in backward manner. Inverse property in this example shows the relationship between the same two instances via property called ‘toProtect’ which means the security requirement are used to protect specific type of context.

Table 2. OWL representation of data inside nodes

<owl:classrdf:ID=”Doctor”> <rdfs:subclassOf> <owl:classrdf:ID=”MedicalProfessional”/> </rdfs:subclassOf> <owl:disjointWith> <owl:classrdf:ID=”Patient”/> </owl:disjointWith> </owl:class>	<RegisteredPatientrdf:about=”#Database”> <hasPatientIDrdf:datatype=http://www.w3.org/2001XMLSchema #string> P301</hasPatientID> <hasPersonNamerdf:datatype=”http://www.w3.org/2001/XMLSchema #string”>John</hasPersonName> </RegisteredPatient>
(a)Class	**(b) Individual**
<owl:DatatypeProperty rdf:about=”#MonthlySalary”> <rdfs:domain rdf:resource=”#TechnicalAssistants”/> <rdfs:range rdf:resource=”http://www.w3.org/2001 /XMLSchema#float”/> </owl:DatatypeProperty>	<owl:objectProperty rdf :about=”hasRequirements”> <rdfs:domainrdf:resource=”#Type of context”/> <rdfs:rangerdf:resource=”#Security requirements”> <owl:inverseOf> <owl:objectProperty rdf:about=”#toProtect”> </owl:inverseOf> </owl:objectProperty>
(c)DataType Properties	**(d)ObjectType Properties**

5. Generalized Framework for Context-aware Security

With the help of ontological method collected data is transferred between various healthcare devices to the knowledge base thereby achieving security of context like patient data by providing deeper insights so as to generate intelligent suggested solutions. A use case scenario in Fig.3 has been generated for a healthcare determining different security requirements of particular context type, the solution type that it interacts with, the solution type internally composed of well-defined architecture with different components, the architecture vulnerable to security attacks threatening one or more security properties and the attacks at different layers having particular security mechanisms to protect their security features.

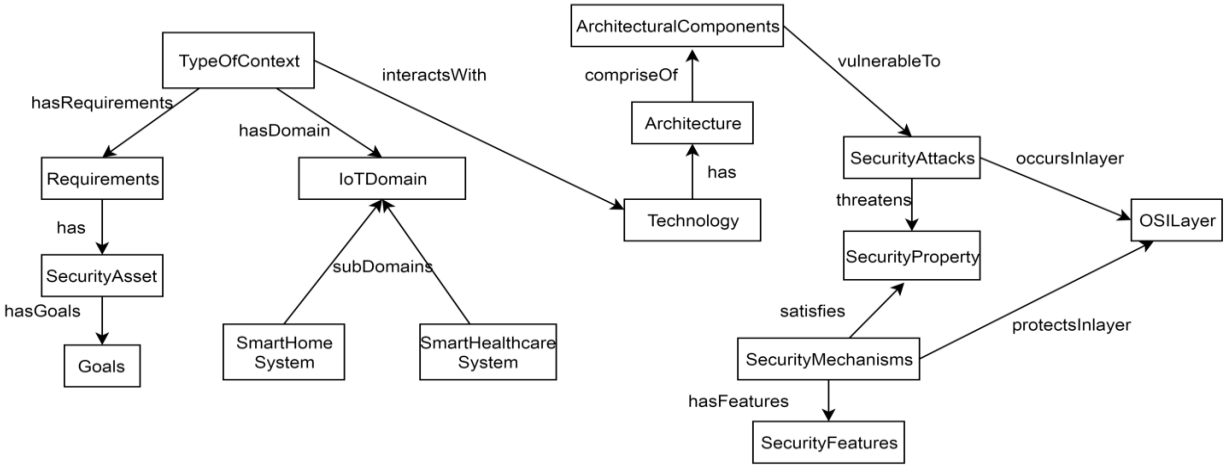

Fig.3.Generalized security framework for IoT

To provide security based on the type of contextual information at particular instant of time, ontology for particular healthcare scenario is generated by identifying various security parameters and their relationship with each other shown in Fig.4. Each arrowed line in the figure defines the subclass association with the main/superclass. We have used STAC ontology to construct our healthcare ontology. Relationship between various security concepts like cryptographic concepts, security protocols, security tools etc. is specified thereby classifying attacks and countermeasures specific to domain knowledge and OSI layer. This security ontology can be reused in different IoT domains (smart transportation system, smart healthcare environment, smart home etc.) where security is the heart of the topic. Further, interested users can access STAC ontology online [http://securitytoolbox.appspot.com/stac.owl] and can be used by any individual in need to secure particular contextual environment.

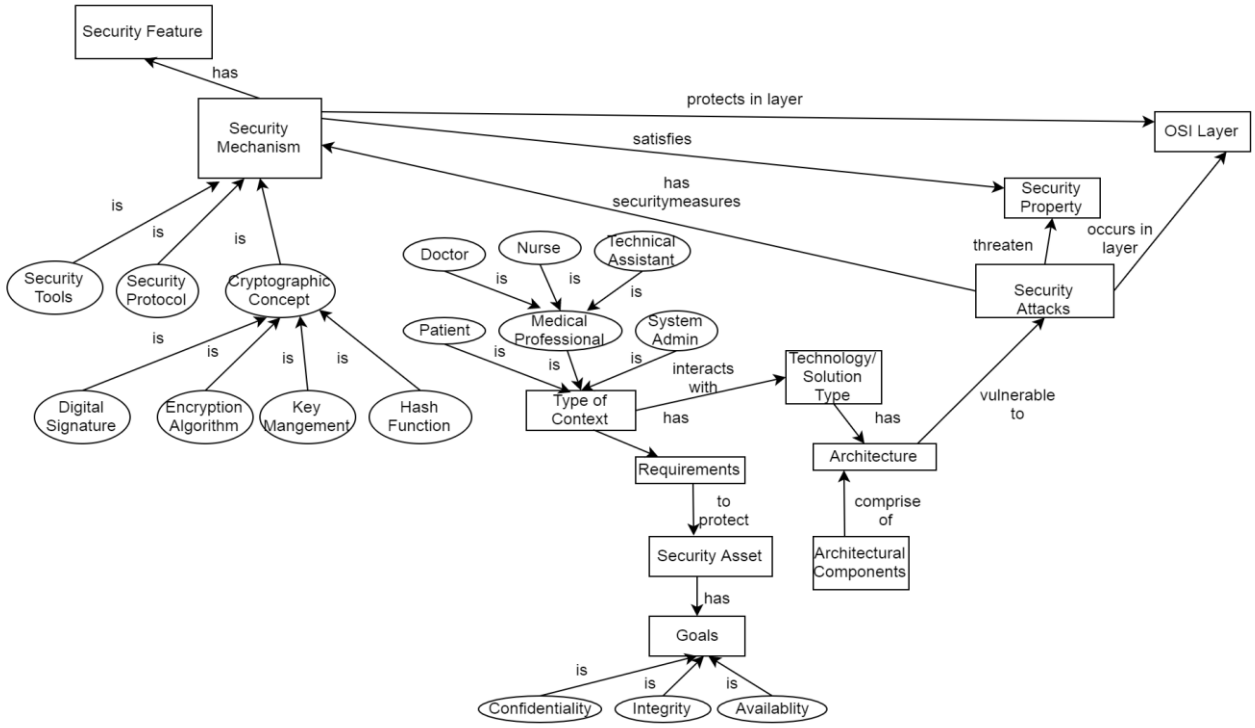

Fig.4. Generating Use-case Scenario for healthcare system

SWRL (semantic web rule language) and SPARQL queries are generated to provide personalized services reducing the workload of medical professionals (checking validation of connected devices) by obtaining valuable knowledge about security assets of the context of interest. SWRL are used to provide definition of different inference rules with regards to present contextual situation. Like the relational database, table are queried using SQL the triples in semantics are queried using w_3c standard SPARQL.SPARQL selects data from the query set by using SELECT statement to conclude which subset of the selected data is to be returned. Further, SPARQL uses a WHERE clause to outline the graph patterns and find a match for in the query dataset [39,40].Fig.3 shows the generalized scenario in IoT while providing security mechanism and Fig.4 shows particular scenario (healthcare) in IoT.

6. Implementation and Evaluation of Use-case Scenario using Protégé

This paper focuses on context-aware security of healthcare domain for effective management of IoT based systems. In this section we show implementation of the generated use-case scenario in Fig.5 using Protégé tool. Further, we developed emergency ontology based upon the context to provide urgent emergency services for people's safety. Emergency services include speedy decision-making, timely service interventions with quick transportation to nearest hospital. For example, people face severe problems in road accident case because of the delayed and inefficient knowledge at hand. In such cases we need quick knowledge sharing among various entities involved, as an inefficient and improper knowledge sharing may lead the life of people in risk. In order to quickly interpret and share data among entities, semantic web and ontology plays very significant role. To share information among different entities in any domain, ontology defines a common vocabulary enabling entities to exchange semantics along with well-defined syntax. Our work provides a base for ontology development and can prove significant contribution for naive users giving full understanding of knowledge sharing among various devices in context.

Protégé is free and open-source ontology editor and framework used for building logical systems [41]. Ontologies are used to describe concepts and relationship between those concepts related to domain of interest. Various ontology languages like RDF, OWL etc. provide different facilities. In this project we use OWL to describe our concepts because of the rich presence of operators such as intersection, union and others. It defines complex concepts in more simplified and logical manner. Because of the presence of logical modelling in OWL, the reasoner can check the mutual consistency of developed ontology maintaining the correctness of hierarchy.Fig.5 shows implementation of our use-case scenario using Protégé with different classes, subclasses, their properties (object properties, data properties) and association between them. Topmost class in protégé is "Thing class" which is the superclass of all the other classes.Fig.6 shows complete implementation of emergency healthcare ontology using protégé comprising of different classes like Devices, Role, Diagnosis, PatientDetails, StaffQualification with subclasses such as thermometer, BP sensor, Degree, HeartAttack etc.

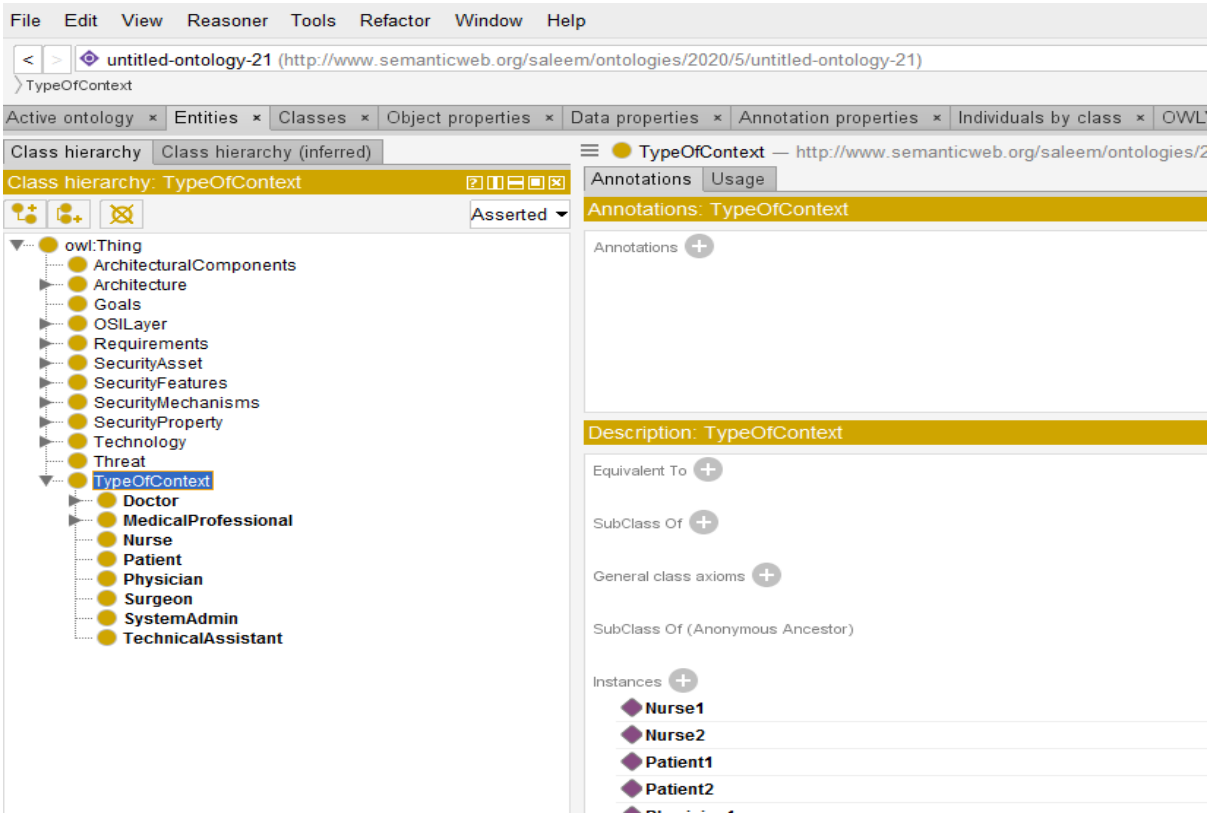

Fig.5. Context-aware healthcare security ontology development

The security ontology developed is incorporated with context-aware security rules providing better reasoning capability and hence make knowledge-aware decisions. The input scenario comprising of particular type of context (patient, medical professional, system admin), architecture and specific technology solutions is feed to protégé After ontological processing of input scenario along with well-defined context-aware rules, an output from protégé identifies potential security issues if any along with corresponding recommended measures. An ontology based approach models and accesses knowledge into a structured description of healthcare system composed of real world entities, data properties, object properties and relationships between them.

The main components in OWL ontology are classes, properties (object properties, data properties) and individuals. OWL classes are defined as set of individuals. In our healthcare ontology different classes are TypeOfContext, Architecture, SecurityMechanisms etc. Individuals represent instances of class in particular domain of interest ,for example in our case subclasses(Patient, MedicalProfessional, SystemAdmin) of class TypeOfContext consist of individuals patient1,Nurse1,TechnicalAssistant1,Surgeon1,Physician1 etc. We use object properties tab to define relationship between individual instances of class and data properties tab to relate individual class instance with literal value (name, surname, age) .To add object property in our ontology, we have object properties tab where topObjectProperty is superclass of all the object properties. In the same way topDataProperties class defines superclass of data properties.

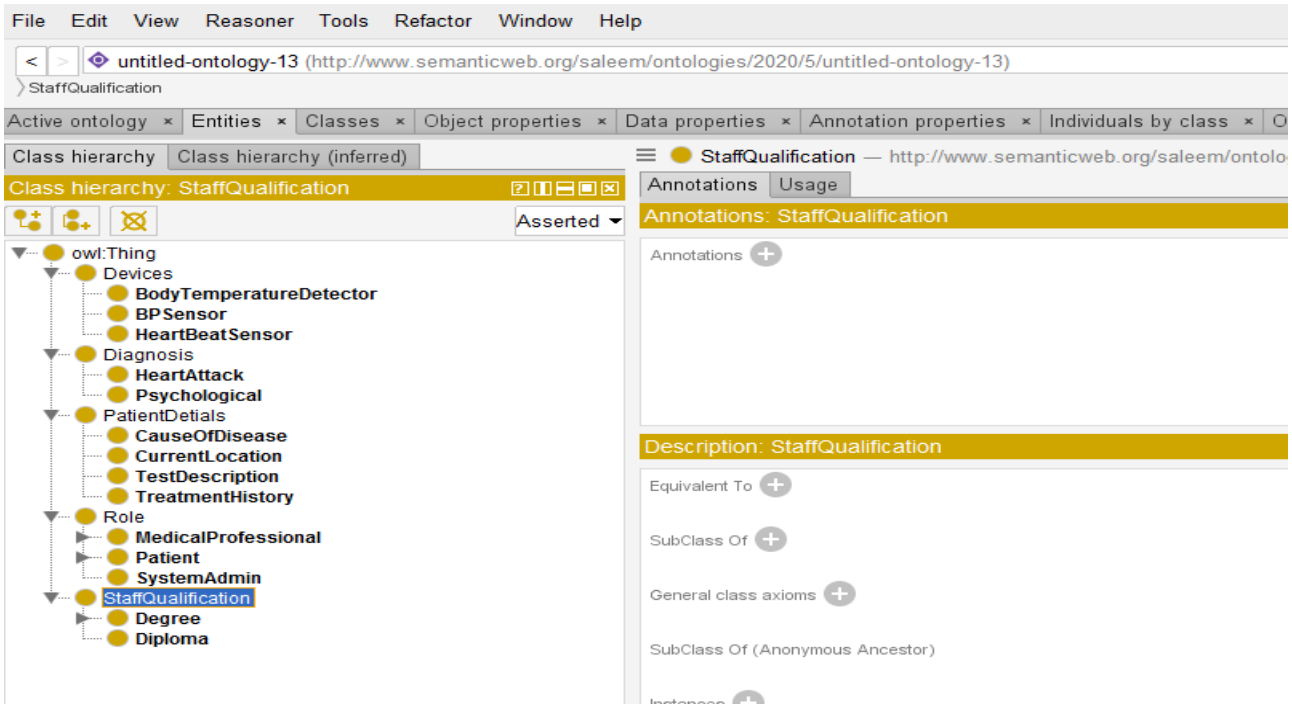

Fig.6.Concepts classification tree in Protégéeditor for Emergency ontology

Fig.7 shows graphical representation of our healthcare ontology relating different concepts implemented using protégé5.The arrows in the figure show association between various classes and subclasses. Also, different coloured arcs in the graph give description of specific relationship types shown in Fig.8.

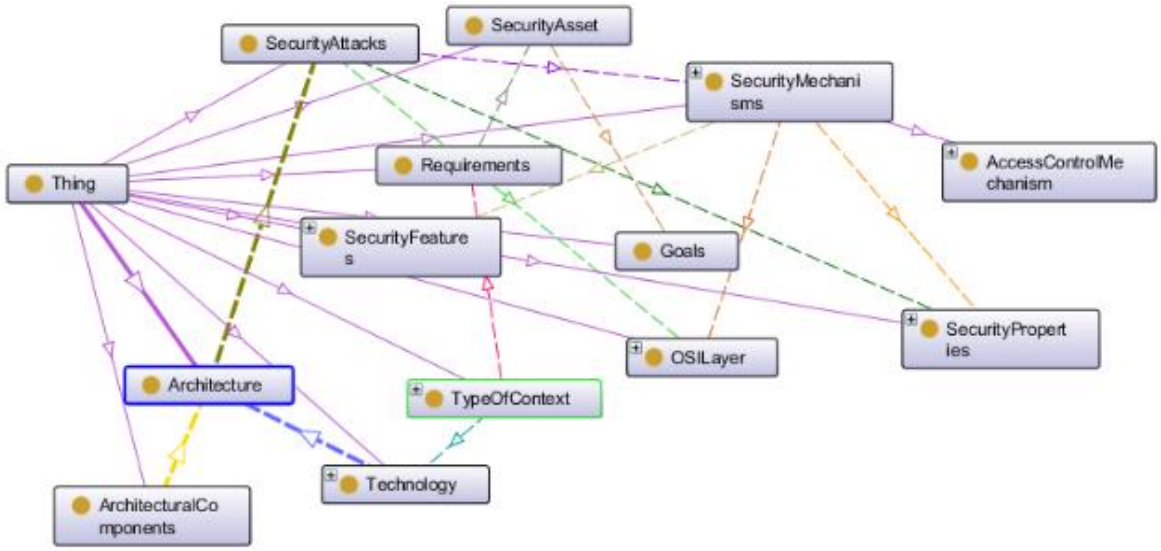

Fig.7. Graphical representation of healthcare ontology

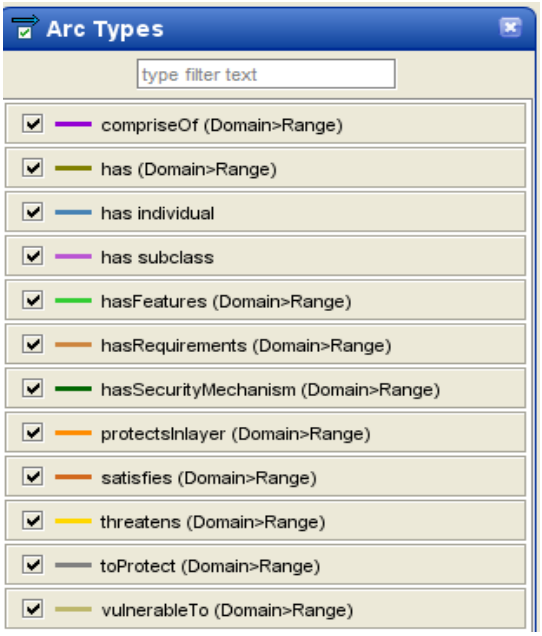

Fig.8.Arc types description

The above figure shows description of different coloured arcs representing diverse information like compriseOf is object type property defining relationship between Architecture and ArchitecturalComponents. Various security mechanisms are used to provide security related to particular attack. SecurityMechanism is defined as a superclass of all subclasses such as SecurityProtocols, CryptographicConcepts, AuthenticationMechanismetc.The graph of emergency ontology created using OntoGraf tab of prot ég éis shown below:

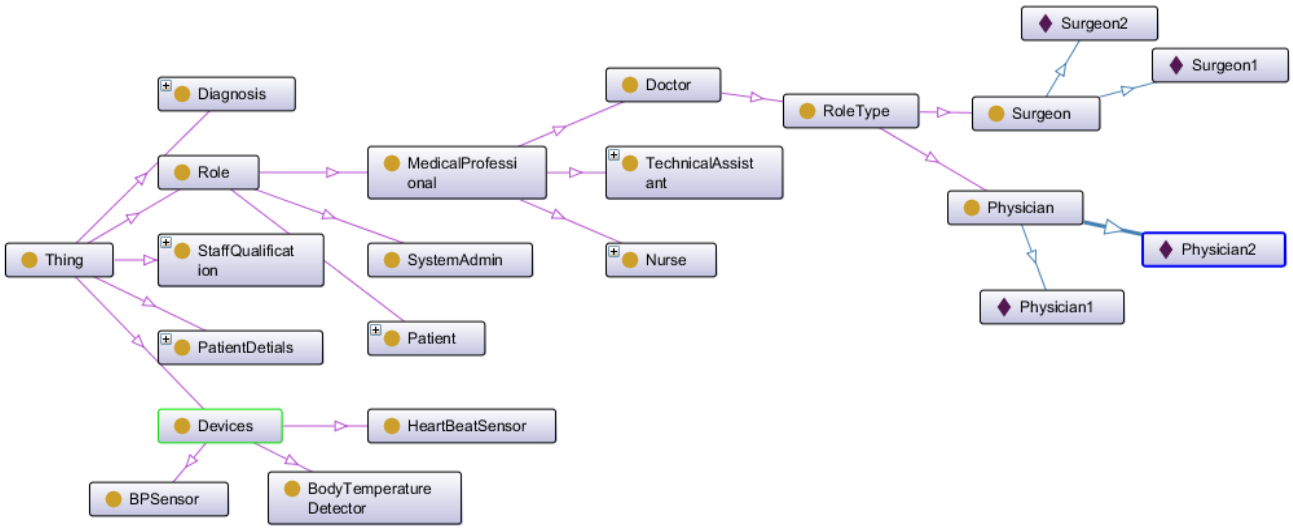

Fig.9. Creating emergency ontology using prot ég é

In this figure class “Thing” is the superclass to which all the other classes are subclasses. Here the nodes with circle type shape inside show either class or subclass, whereas nodes with diamond shaped structure indicate individuals of classes of subclasses. We can assert properties on individual instance of class according to specific need. One of the main properties inherited by OWL-DL is that their processing is performed by reasoner. The feasibility and consistency checking of ontologies is very important as it finds out if any duplicate instances are present that may decrease the significance of ontology. One of the main facilities offered by reasoner is its ability to check whether one class is subclass of another which is performed by computing inferred class hierarchy. Other special service that is offered by reasoner is process of consistency checking which is done based on the description logic of various classes and hence conclusion is made whether the defined class can have such instances. A class is reasoned to be inconsistent if it cannot infer the expected results and reasoner will show related error message once executed. Table3 gives description of various threats affecting specific security properties at three layers of IoT with corresponding counter-measures.

Table 3. Attacks with corresponding counter-measures at each layer

Threat	Layer	Type of Context	Affecting security property	Protocols	Architecture Type	Counter-measure
CoAP exploit	Application layer	Personal health records of patient, Eavesdropping on patient's location, Compromising devices connected to patient	Authentication, Authorization, Confidentiality	CoAP, DDS, MQTT, SMQTT, AMQP	Stationary, Cloud-based, wearable, Implantable	CoAPs, employment of DTLS
False data injection						Collective secret
Path-based DoS						One-way hash chains
Sinkhole	Network layer	Unauthorized entities accessing system's resources, Weak authentication between IoT devices, System admin storing data in insecure fashion	Integrity, Authentication	6Lowpan, RPL, CORPL, CARP, 6TISCH	Wearable , Stationary Gateway dependent	Secure routing algorithm
Sybil						Indirect validation , ID-based public keys
Wormhole						Location-based keys, DAWWSEN
Jamming-DoS	Perception layer	Weak or guessable password of devices in communication between patient and doctor, Modification of nodes involved in data transfer	Authentication, Integrity	LTE-A, Z-Wave, Zigbee smart, DASH7, 802.11ah	Stationary mobile controlled, Stationary gateway dependent	Swarm intelligence
Tampering						Routinely executing physical checks
Eavesdropping						Key pre-distribution

Let us consider a scenario to explain how counter-measures are suggested by incorporation of rules with regards to particular scenario. A scenario is contemplated where the security asset to be secured is patients data with the identified attack as Sybil attack occurring at network layer which may affect integrity and authentication of data. With the process of following:

threatens(?t,?a)^hasSecurityMechanism(?t,?sm)->thwarts(?sm,?a) rule incorporation on this scenario the security mechanisms suggested for Sybil attack are Indirect validation and ID-based public keys. Same process applies for all the other real case scenarios.InFig.10 code snippets regarding object property assertions and data property assertions are shown. Its explanation has already been defined in Table2. Fig.10(a) show code snippet describing assertion of different object properties with corresponding domain and range. In Table(b) code snippet explaining assertion of data properties like first name, last name etc. is explained.

In protégé an ontology that is constructed by ones mutual understanding is called the asserted hierarchy whereas the class hierarchy that is automatically generated by reasoner is known as inferred hierarchy. Classify button is used by reasoner to automatically invoke the action of reasoning and once an inferred hierarchy is computed, an inferred hierarchy window pops open on top the manually constructed hierarchy window. This process of computing an inferred class hierarchy from asserted class hierarchy is known as classifying ontology. To evaluate and check such inconsistencies we perform reasoning on descriptive logic reasoner. We can use different reasoning tools like Pellet, HermiT, Racer, FACT++ to check consistency of our developed OWL ontology along with set of class, subclass, object properties, data properties descriptions performing intelligent reasoning [42,43]. If a class is found to be inconsistent then its icon will be highlighted with red colour. We used Pellet (Incremental) reasoner to evaluate our ontologies because of its relatively easy interface with Protégé.

To query our OWL ontology, firstly query is send to the reasoner to check consistencies of ontology and accordingly returning error or ok message to the requester. Our evaluation has proved successful indicating that our concept is reliable offering annotated recommendations requiring less human-intervention. Our work provides a conceptual view of how knowledge sharing can ease the contextual situations efficiently in timely manner.

```
<ObjectPropertyDomain>
    <ObjectProperty IRI="#compriseOf"/>
    <Class IRI="#ArchitecturalComponents"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#has"/>
    <Class IRI="#Technology"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#hasFeatures"/>
    <Class IRI="#SecurityMechanisms"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#hasGoals"/>
    <Class IRI="#SecurityAsset"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#hasRequirements"/>
    <Class IRI="#TypeOfContext"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#hasSecurityMechanism"/>
    <Class IRI="#SecurityAttacks"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#interactsWith"/>
    <Class IRI="#TypeOfContext"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#occursInlayer"/>
    <Class IRI="#SecurityAttacks"/>
</ObjectPropertyDomain>
```

(a)ObjectProperty assertion

```
<DataPropertyAssertion>
    <DataProperty IRI="#First_Name"/>
    <NamedIndividual IRI="#Nurse1"/>
    <Literal datatypeIRI="&xsd;string">Ananya </Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#Last_Name"/>
    <NamedIndividual IRI="#Nurse1"/>
    <Literal datatypeIRI="&xsd;string">Singh</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#Staff_Id"/>
    <NamedIndividual IRI="#Nurse1"/>
    <Literal datatypeIRI="&xsd;integer">7839</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#First_Name"/>
    <NamedIndividual IRI="#Nurse2"/>
    <Literal datatypeIRI="&xsd;string">Rahul</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#Last_Name"/>
    <NamedIndividual IRI="#Nurse2"/>
    <Literal datatypeIRI="&xsd;string">David</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#Staff_Id"/>
    <NamedIndividual IRI="#Nurse2"/>
    <Literal datatypeIRI="&xsd;integer">7643</Literal>
</DataPropertyAssertion>
```

(b)DataProperty assertion

Fig.10. Code Snippets

7. Conclusion

IoT is a system of interconnected devices that has numerous application domains like smart agriculture system, smart home management etc. Due to dynamic contextual situations in IoT, static approaches for security is infeasible. Therefore, non-static or context-aware approaches become essential for any IoT domain to provide better security amenities. In this work we have used STAC ontology as a base to develop our security ontology for healthcare environment. Moreover, emergency ontology that can prove useful during difficult times has been constructed. Ontological engineering in combination with context-aware rules have been incorporated to provide security in healthcare domain. We throw light on importance of context-awareness in IoT to achieve secure communication between IoT nodes. The implementation of this work is done using Protégé tool and evaluation is performed on Pellet (Incremental) reasoner. Implementation of use-case scenario in diagrammatical form upon rule incorporation determine security requirements specific to present condition and suggest intelligent solutions accordingly. Our work can enable naïve security ontology developers, helping them to understand conceptual overview of semantics and security ontologies in a comprehensive manner. Security mechanisms adaptable to dynamic context such as authentication mechanisms involving face recognition, biometric or iris scanner can represent a promising direction.

Acknowledgement

This research work is funded under the seed grant initiative of TEQIP-III project currently being implemented at Islamic university of Science and Technology, Awantipora, Jammu and Kashmir.

References

[1] Zheng Yan, Xixun Yu, And Wenxiu Ding, "Context-Aware Verifiable Cloud Computing", *IEEE Access*, 2017, Vol. 5, pp. 2211-2227.

[2] Evdokimov, I.V., Alalwan, A.R.J., Tsarev, R.Y., Yamskikh, T.N., Tsareva, O.A. and Pupkov, A.N., 2019, March. A cost estimation approach for IoT projects. In *Journal of Physics: Conference Series* (Vol. 1176, No. 4, p. 042083). IOP Publishing.

[3] Bassi, A., Bauer, M., Fiedler, M., van Kranenburg, R., Lange, S., Meissner, S. and Kramp, T., 2013," *Enabling things to talk* ",Springer Nature,2013, p. 379.

[4] Perera, Charith, ArkadyZaslavsky, Peter Christen, and DimitriosGeorgakopoulos. "Context aware computing for the internet of things: A survey." *IEEE communications surveys & tutorials*, 2013, Vol.16, no. 1,pp.414-454.

[5] B. Schilit and M. Theimer, "Disseminating active map information to mobile hosts", *Network, IEEE Network,*sep/oct 1994, vol. 8, no. 5, pp. 22 –32.

[6] N. S. Ryan, J. Pascoe, and D. R. Morse, "Enhanced reality fieldwork: the context-aware archaeological assistant" ,*In Computer Applications in Archaeology 1997, ser. British Archaeological Reports, V. Gaffney, M. van Leusen, and S. Exxon, Eds. Oxford: Tempus Reparatum*, October 1998.

[7] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," *In Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing, ser. HUC '99. London, UK: Springer-Verlag*, 1999, pp. 304–307.

[8] Dey, A.K.,"Context-aware computing: the CyberDesk project", *Proceedings of the AAAI 1998 Spring Symposium onIntelligent Environments*, 1998, pp.51–54.

[9] Brown, P.J. ,"The stick-e document: a framework for creating context-aware applications", *Proceedings of theElectronic Publishing*, Palo Alto, 1995 ,pp.259–272.

[10] Dey, A.K. and Abowd, G.D. ,"Towards a better understanding of context and context-awareness", *Proceedingsof the Workshop on the What, Who, Where, When and How ofContext-Awareness*, ACM Press, New York,2000b

[11] Hofer, T., Schwinger, W., Pichler, M., Leonhartsberger, G. and Altmann, J. ,"Context-awareness on mobile devices – the hydrogen approach", *Proceedings of the 36thAnnual Hawaii International Conference on System Sciences*, 2002 ,pp.292–302

[12] P. Hu, J. Indulska, and R. Robinson, " An autonomic context management system for pervasive computing," ." In *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2008, pp. 213–223

[13] K. Henricksen, "A framework for context-aware pervasive computing applications," *Computer Science, School of Information Technology and Electrical Engineering, The University of Queensland*, September 2003

[14] Strang, Thomas, and Claudia Linnhoff-Popien."A context modeling survey."*In Workshop Proceedings.*2004.

[15] Korpipää, P. and Mäntyjärvi, J. (2003) "An ontology for mobile device sensor-based context awareness",*Proceedings ofCONTEXT, 2003, Vol. 2680 of Lecture Notes in ComputerScience*, pp.451–458.

[16] K.-E. Ko and K.-B. Sim, "Development of context aware system based on bayesian network driven context reasoning method and ontology context modelling",*In 2008 International Conference on Control*, Automation and Systems,2008,pp.2309-2313.

[17] R. de FreitasBulcaoNeto and M. da Graca Campos Pimentel, "Toward a domain-independent semantic model for context-aware computing" ,In Third Latin American Web Congress LA-WEB 2005), 2005, p.10 -pp.

[18] M. Compton, C. Henson, H. Neuhaus, L. Lefort, and A. Sheth, "A survey of the semantic specification of sensors", *In 2nd International Workshop on Semantic Sensor Networks, at 8th International Semantic Web Conference*, Oct. 2009.

[19] ArbiaRiahiSfar , Enrico Natalizio, YacineChallal , ZiedChtourou , "A roadmap for security challenges in the Internet of Things", *Digital Communications and Networks*, Vol.4,no.2 ,2018 Vol.9pp.118–137

[20] P. A. Laplante, M. Kassab, N. L. Laplante, and J. M.Voas, ``Building caring healthcare systems in the Internet of Things',' *IEEE Syst. J.* , Sep. 2018., vol. 12, no. 3, pp. 3030-3037

[21] Herzog, Almut, NahidShahmehri, and Claudiu Duma. "An ontology of information security", *International Journal of Information Security and Privacy (IJISP*), 2007, Vol.1, no. 4 1-23.

[22] R. M. Savola, P. Savolainen, A. Evesti, H. Abie, and M. Sihvonen, "Risk driven security metrics development for an e-health IoTapplication*",InProc. Inf. Secur. South Afr. (ISSA)*, Aug. 2015, pp. 1-6.

[23] Mozzaquatro, Bruno Augusti, Carlos Agostinho, DiogoGoncalves, João Martins, and Ricardo Jardim-Goncalves. "An ontology-based cybersecurity framework for the internet of things." *Sensors*,2018 ,Vol.18, no. 9,p.3053

[24] Gonzalez-Gil, P., Martinez, J.A. and Skarmeta, A.F., "Lightweight Data-Security Ontology for IoT", *Sensors*, 2020. Vol.*20*,no.3, p.801.

[25] Ayele, Getinet. "Semantic description of IoT security for smart grid.",*Master's thesis, Universitetet i Agder; University of Agder*, 2017.

[26] Food and Drug Administration, "Postmarket Management of Cybersecurity in Medical Devices", *Silver Spring: Food and Drug Administration*, 2016

[27] Naval Medical Logistics Command, *Medical Device Risk Assessment Questionnaire Version3.0*,2016

[28] Salini, P., and S. Kanmani. " Ontology-based representation of reusable security requirements for developing secure web applications." *International Journal of Internet Technology and Secured Transactions*, 2013, *Vol.* 5, no. 1 ,pp. 63-83.

[29] Busch, Marianne, and Martin Wirsing. "An Ontology for Secure Web Applications", *Int. J. Software and Informatics*,2015, Vol.9, no. 2 pp. 233-258.

[30] S. E. Parkin, A. van Moorsel, and R. Coles, "An information security ontology incorporating human-behavioural implications", *In Proceedings of the 2nd International Conference on Security of Information and Networks. ACM*, 2009, pp. 46–55.

[31] Tao, Ming, JinglongZuo, Zhusong Liu, Aniello Castiglione, and Francesco Palmieri. "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes." *Future Generation Computer Systems*, 2018, Vol.78 pp.1040-1051.

[32] B. A. Mozzaquatro, R. Jardim-Goncalves, and C. Agostinho, "Towards a reference ontology for security in the Internet of Things", *2015 IEEE International Workshop on Measurements and Networking, M and N 2015 - Proceedings*,2015, pp. 117–122

[33] F. de Franco Rosa, M. Jino, and R. Bonacin, "Towards an Ontology of Security Assessment: A Core Model Proposal," *In Advances in Intelligent Systems and Computing*, vol. 738, 2018, pp. 75–80.

[34] Daniele, L., Costa, P.D. and Pires, L.F., 2007, July. Towards a rule-based approach for context-aware applications.In *Meeting of the European Network of Universities and Companies in Information and Communication Engineering* (pp. 33-43).Springer, Berlin, Heidelberg.

[35] Horrocks, I.; Patel-Schneider, P.F.; Boley, H.; Tabet, S.; Grosof, B.; Dean, M. SWRL: A Semantic Web Rule Language Combining OWL and RuleML. Available online: http://www.daml.org/rules/proposal/(accessed on 16 January 2018).
[36] Sirin, E.; Parsia, B.; Grau, B.C.; Kalyanpur, A.; Katz, Y. Pellet: A practical OWL-DL reasoner. Web Semant. Sci. Serv. Agents World Wide Web **2007**, 5, 51–53. [CrossRef]
[37] Zhang, F., Wang, K., Li, Z. and Cheng, J., 2019. Temporal Data Representation and Querying Based on RDF. *IEEE Access*, *7*, pp.85000-85023.
[38] de Laborda, Cristian Pérez, and Stefan Conrad. "Relational. OWL: a data and schema representation format based on OWL." In *Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling-Volume 43*, pp. 89-96. 2005
[39] Lawan, Abba, and AbdurRakib. "The semantic web rule language expressiveness extensions-a survey." *arXiv preprint arXiv:1903.11723* (2019).
[40] Kollia, I., Glimm, B. and Horrocks, I., 2011, May. SPARQL query answering over OWL ontologies. In *Extended Semantic Web Conference* (pp. 382-396).Springer, Berlin, Heidelberg.
[41] Gennari, John H., Mark A. Musen, Ray W. Fergerson, William E. Grosso, Monica Crubézy, Henrik Eriksson, Natalya F. Noy, and Samson W. Tu. "The evolution of Protégé: an environment for knowledge-based systems development." *International Journal of Human-computer studies* 58, no. 1 (2003): 89-123.
[42] Bock, Jürgen, Peter Haase, QiuJi, and Raphael Volz. "Benchmarking OWL reasoners." In *ARea2008-Workshop on Advancing Reasoning on the Web: Scalability and Commonsense*. Tenerife, 2008.
[43] Glimm, Birte, Ian Horrocks, Boris Motik, GiorgosStoilos, and Zhe Wang. "HermiT: an OWL 2 reasoner." *Journal of Automated Reasoning* 53, no. 3 (2014): 245-269.

Authors' Profiles

Asifa Nazir received her bachelor's degree in Computer Science & Engineering from University of Kashmir, Srinagar, J&K in 2015. Next, she received her Master's degree in Information Technology from Central University of Kashmir, Srinagar, J&K in 2018.Currentlly, she is working as a Research Assistant at Islamic University of Science & Technology, Awantipora, J&K in the department of Computer Science & Engineering. Her research interests are IoT, Artificial Intelligence, Network Security and Wireless Sensor Networks.

Sahil Sholla, is Assistant Professor at department of Computer Science & Engineering, Islamic University of Science and Technology Awantipora, Pulwama , J&K, India .He has received PhD from National Institute of Technology Srinagar, India. His research focuses on technology ethics, security and Internet of Things**.**

Adil Bashir received his Bachelor of Technology (B.Tech) in Computer Science and Engineering from Islamic University of Science and Technology, Jammu & Kashmir, India in year 2011. He has done his Master of Technology (M.Tech) in Communication and Information Technology from National Institute of Technology (NIT) Srinagar, India in 2013. Presently he is Assistant Professor in Computer Science and Engineering department at IUST Awantipora, Jammu and Kashmir, India. His areas of interest are Internet of Things, Wireless Sensor Networks, Embedded Systems and Network Security.

How to cite this paper: Asifa Nazir, Sahil Sholla, Adil Bashir, " An Ontology based Approach for Context-Aware Security in the Internet of Things (IoT)", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.1, pp. 28-46, 2021.DOI: 10.5815/ijwmt.2021.01.04