UNIVERSITETET I AGDER

Semantic Description of IoT Security for Smart Grid

GETINET AYELE ESHETE

JAN PETERSSEN NYTUN
HABTAMU ABIE

University of Agder, June 2017
Faculty of Engineering and Science
Department of Information and Communication Technology

Abstract

This research work proposed, developed and evaluated IoT Security ontology for smart home energy management system (SHEMS) in smart grids. The ontology description includes infrastructure, attacks, vulnerabilities and counter measures for the main components of SHEMS such as Smart Meter, Smart Appliance, Home Gateway, and Billing data. The ontology extends the SAREF energy management ontology with security features. We have two main reasons for selecting SAREF ontology to base our work on. First, SAREF is standardized by ETSI. Second, it is specifically designed for energy management and efficiency. We checked the correctness of our ontology by running SWRL rules and SPARQL queries. Our test results showed that our ontology is useful to analyse and infer IoT security for smart home and can be extended to more complex reasoning of IoT security features.

Keyword: IoT, Security, Smart Grid, Smart Home, Energy Management

Preface

This master thesis is submitted in partial fulfilment of the requirements for the degree of Master of Science in Information and Communication Technology at the University of Agder, Faculty of Engineering and Science. The work has been conducted at Norwegian Computing Center(NR) under the IoTSec project. The IoTSec - Security in IoT for Smart Grids initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) to contribute to a safe information society. Associate Professor Jan Nytun has been the thesis supervisor at UiA and Chief Research Scientist Habtamu Abie has been the supervisor from the NR.

Acknoledgement

I greatly thank the Norwegian Computing Centr(NR) for giving me the opportunity to do my Master's thesis under IoTSec project. I highly acknowledge my supervisor Jan Pettersen Nytun, and my NR supervisor Chief Scientist Habtamu Abie for their excellent and constructive supervision throughout this research work.

I would also like to express my sincere thanks to my wife, my baby and to all families for their love and advice.

.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

SHEM - Smart Home Energy Management

HEM - Home Energy Management

IoT – Internet of Things

HG – Home Gateways

ETSI – European Telecommunication Standard Institute

DR – Demand Response

NIST - National Institute of Standards and Technology

MSDL - Microsoft’s security development lifecycle

Chapter 1

1 Introduction

Internet of things (IoT) is a technology that links objects that are connected to the internet and let these objects communicate each other. It includes devices, actuators, sensors, appliances, and others connected to the internet [1]. Almost all application domains such as health, transport, energy, business, and entertainment are using IoT [2]. Cisco predicted over 50 billion devices will be connected to the internet in 2020 [3].

Smart Grid is one of IoT application areas becoming popular and successful. According to IHS market prediction, Smart Grid Sensors market will generate $350 billion in 2021 [4] and Smart Grid Security will worth $7 billion in 2021 [5]. Smart Grid consists of billions of smart objects such as smart appliances, smart meters, actuators, sensors, etc. Even if the adoption of IoT devices in Smart Grid is increasing, there are several issues to be addressed. Few of the challenges include identifying all objects connected to the internet, interoperability between objects, security and privacy of the information flow.

According to Friess [6] semantic technologies can play a great role on describing, linking and reasoning IoT concepts across utilities, enterprises, and applications. The dynamicity of two-way information flow from IoT devices to the gateway then to the destination from millions and billions of heterogeneous devices makes hard to detect the security breaches on real time bases. When the infrastructure is sensitive like Smart Grid, the security models and systems should estimate and predict contextual changes in their environments, and adapt their security decisions upon those estimates and predictions [7]. This thesis focuses on the use of the Semantic Web technologies to develop ontologies to improve the prediction and assessment of security of IoT in the Smart Grid.

Our security ontology has been developed based on the security relationship model described in the National Institute of Standards and Technology Special Publication 800-12 [8].

1.1 Aims and Objectives

The aim of this thesis is to analyze the smart energy infrastructure, attacks and counter measures and from the result of the analysis, build an ontology to improve the prediction and assessment of security of IoT in the Smart Grid. To achieve this the main objectives of this thesis are as follows:

- Analyse the requirements of IoT security in Smart Energy Management System.
- Review available ontologies related to IoT and Security.

- Compare the ontologies, select, adopt and extend the selected ontology to our work.
- Select development tool that is suitable and appropriate for our project.
- Develop the ontology that incorporates IoT security in Smart Grid.
- Evaluate the ontology by running queries.

1.2 Research Challenges

Most of European countries will replace the traditional Electric Meter to Smart Electric Meter in the coming 3-5 years. For example, Norway will replace all traditional Electric Meter to Smart Meter in 2019 and Netherland in 2020. Even if the Adoption of IoT enabled Smart Grid is increasing in the last decade, there are several challenges in assuring the Security and Privacy of IoT ecosystem in Smart Grid:

- Several parameters such as the type of network, IoT Environment, Communication technologies, etc. need to be considered
- Millions and billions of small to large heterogeneous objects send and receive data in real-time bases.
- The security mechanism should learn the context of the dynamic environment of IoT.

1.3 Structure of the thesis

The structure of the remaining part of the thesis is as follows:

- Chapter 2 gives the background of IoT and its application, highlights the state of the art of Smart Grid and Smart House, and reviews ontologies a solution to IoT Interoperability and Security. The chapter also reviews the background of Semantic web technologies.
- Chapter 3 describes the details of the main components of the elected scenarios such as Home Energy Management System, Smart Meter, Smart Appliance, and Home Gateway from the perspective of IoT Security. The chapter presents the ontology architecture.
- Chapter 4 describes the implementation of the main components of the proposed ontology applied to the scenario. The Ontology of the System is developed by following Ontology engineering rules. The chapter discusses how our implementation has met its objectives by inferencing the Knowledges of the Ontology.
- Chapter 5 concludes the thesis and points out future work.
- Chapter 6 presents the Reference Materials used in the thesis.

Chapter Two

2 Background and Literature Review

2.1 Introduction

This chapter has three main parts. The first part reviews the background of Semantic Web technologies. The second part describes IoT and its application; Smart Grid and Smart House; the technologies used in Smart Grid and Smart house. The last part reviews related works; IoT Security, IoT Ontologies and Security Ontologies as shown from figure 2-1 below. Semantic web gives brief background and description about Semantic technologies such as Ontology, Ontology Language and Ontology development tools. The IoT section describe about the definition and application of IoT in Smart Grid and Smart House. The last section of the chapter describes about Ontologies related to IoT interoperability and IoT Security. At the end of each section we compared the technologies based on selected parameters which helps us in selecting the best candidate technologies we used in our paper.

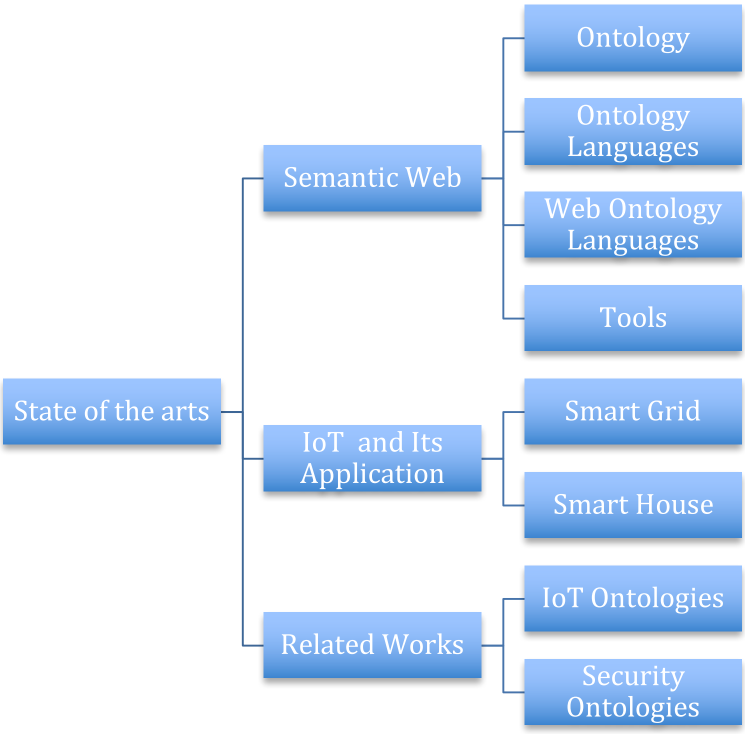


Figure 2-1: Structure of State of the Art

2.2 Semantic Web

Semantic web refers to an extension of the current web through use of different standards supported by the World Wide Web consortium (W3C), which allows exchange of protocols and support common data formats [9].

Major difference that differentiates semantic web technologies from other data technologies such as World Wide Web and relational databases is that it deals with the meaning of data [10]. The semantic web technologies give us the opportunity to create web data stores, create rules for the data handling and build vocabularies. Such technologies include: Resource Description Framework (RDF), SPARQL Protocol and RDF Query Language (SPARQL), SWRL, and Web Ontology Language (OWL)[11] .

2.2.1 Ontology

Ontology refers to the description of concepts and the relationship that exists in the domain of interest [12]. The concepts are used for the purpose of representing knowledge and properties. Generally, ontology is used to serve various purposes in sharing information since different people have different needs to be met. It allows reusability of the already existing knowledge thus there is no need to develop new ontology from scratch. It has the concepts to define set of entities existing and their relationship in a domain. It allows knowledge sharing between semantic independent readers.

2.2.2 Ontology languages

These refer to formal languages that are used in the process of creating ontologies. They allow encoding of specific domain knowledge and support reasoning rules for the knowledge processing [12]. The use of different languages is defined by the kind of application to be developed and any modifications that may be necessary. The ontology languages include:

2.2.3 Resource Description Framework (RDF)

This is a data model language used in representing resources in the web and has features that support merging of data despite the differences that exist in the underlying schemas. It supports schema evolution without the need to change all data consumers. This data model language helps in making resource statements in triples form (subject, object and predicate). These triples form graph where nodes are subject and object while predicate represents the edge of the graph [12].

The triples are identified through the use of URI (Uniform Resource Identifier). In this case, the subject represents the resources to be described and can be a blank node or an IRI. The predicate refers to the property of that resource. It describes the binary relationship between subject and object and is always an IRI. The object is the value of the resource which corresponds to intersection of columns and rows in traditional relational database table. This can be a blank node, literal value or an IRI [13].

2.2.4 Web Ontology Language (OWL)

This is a language recommended by W3C designed for semantic web development and is based on description logic. It allows the user to create ontologies that behave like other web documents and its domain can be described in terms of classes, individuals and properties. The **OWL class** groups individuals of similar characteristics into groups and are identified by use of URI through its name. Every class has individuals associated to it and they are called member of that class [12].

Property defines the binary relationship between individuals of classes or between individuals to data value such as integer and string. OWL has three types of properties which include, object property, data-type property and annotation property. The object property normally denoted as owl: **ObjectProperty** relates individual from one class to individual from another class. For instance, **employedAt** can be used to relate individual to a company. The Data-type property normally denoted as Owl: **DatatypeProperty** is used to link a class or individual to a data value. For example: **hasName** is used to relate a person to string. The annotation property is used to add additional information to classes, individuals and properties such as comments and versions. This added information is not interpreted but is there to make the ontology easier for human to understand [13].

Resource Description Framework Schema (RDFS)

This is a recommended data modeling language by W3C that defines the semantic vocabularies for RDF resources and allows definition of ontologies through the definition of classes, taxonomies, properties and relationships existing between classes and properties. Elements of RDFS include:

Rdfs: subClassOf used to indicate that one class is subclass of another class.

Rdfs: subpropertyOf used to indicate that a property is a sub-property of another. It indicates that one property is more specific than another property.

Rdfs: domain and Rdfs: range - are used to describe the property by defining how the property can be used by inferring the number of subject of triples as a member of Class domain.

Rdfs: type - this is used to specify the member of class in a domain.

2.2.5 Ontology Development Tools

There exist various tools for the development of ontology. The most popular ones are:

Protégé: Protégé is an open source ontology editor used in building knowledge based solutions in various specialization areas [13]. It is used in creating and editing ontology components such as properties, classes and individuals. Classes are sets of Individuals in a domain and Domain classes are organized in class hierarchies. Thing is the root class for protégé and Subclasses are specialized forms of their super classes. It supports class axioms for querying and building the class relations [14] .

WebProtégé: This is a free, open source collaborative ontology used as an environment for development of the web. It has editing interface that provides access to commonly used OWL construct. It has revision history and full change tracking. WebProtégé supports editing OWL 2 and OBO ontologies. It consists of collaborative tools like threaded notes and discussions, sharing and permission and watches and email notifications. WebProtégé houses multiple formats for both download and upload of ontologies [15].

NeOn toolkit [16]: It is a state-of-the-art multi-platform open source ontology engineering environment which supports comprehensive ontology life-cycle. The toolkit is based on a leading development environment, Eclipse platform and is used to provide extensive set of plug-ins that covers various ontology engineering elements.

Swoop [17]: This is a hypermedia-based featherweight OWL ontology editor. It is an open source collaborative ontology that has reasoning capabilities. It does not support tracking and versioning.

OWLGrEd: It is an open source UML style graphical editor used in OWL ontology. OWLGrEd has additional elements for graphical ontology development and exploration including interoperability with Protégé [18] .

OntoWiki: This is a front-end application developed for semantic data web to support collaborative knowledge engineering scenarios. It serves as a development framework for applications which are knowledge intensive. OntoWiki Supports navigation by the use of RDF knowledge through SPARQL- generated trees, tables and lists [19]. Resources here are represented automatically in form of hyperlinks and therefore, backlinks are generated when feasible.

MoKi [20] This is an open source ontology tool that is partially collaborative and partially supports threaded discussions. It has reasoning capabilities but lacks tracking and versioning properties.

Tool	Multi User	Distributed/Collaborative	*Threaded Discussions*	*Reasoning capabilities*	Open Source	*Tracking and Versioning*

Protégé		×	×	✓	✓	×
WebProtege	✓	✓	✓	×	✓	✓
NeOn toolkit		×	×	✓	✓	×
Swoop	✓	✓	×	✓	✓	×
OWLGrEd		×	×	×	✓	×
OntoStudio	✓	✓	✓	✓	×	✓
OntoWiki	✓	✓	✓	✓	✓	✓
MoKi	✓	✓	✓	✓	✓	×

Table 1: Comparison between Ontology Development tools

The beginning for the development of our Ontology has started by comparing various ontology development tools based on the parameters shown in table 1. The main aim of the comparison is to select a tool that supports collaborative, threaded discussions, tracking and versioning, and Open Source. Because IoTSec project is planning to develop the full Smart Grid Ontology by its collaborators and all collaborators can add, edit, update, and discuss by having the same ontology file. We selected WebProtégé IDE to develop our ontology which supports collaborative, threaded discussions, tracking and versioning of the ontology.

2.3 IoT

In the last two decades, IoT is becoming one of a trending technology. Even if the number of IoT deployments is exponentially increasing, there is no universal definition and standards. Different technological organizations and Scholars defined IoT in different terms.

Gartner define IoT "*The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."*

IBM also IoT as*:" Internet of Things, or IoT, refers to the growing range of Internet-connected devices that capture or generate an enormous amount of information every day. For consumers, these devices include mobile phones, sports wearables, home heating and air conditioning systems, and more. In an industrial setting, these devices and sensors can be found in manufacturing equipment, the supply chain, and in-vehicle components."*

According to Ghidini, et al. [20] the application domains of IoT can be classified into four broad Personal and home (Smart House), Utilities (Smart Grid, Smart Meter), Enterprise, and Transport and Logistics. This thesis focuses on Smart Grid and Smart House application domains.

2.3.1 Smart Grid

According to the U.S Government's International Energy Outlook 2016, world energy consumption is projected to increase by 48 percent from 2012 to 2040[1]. U.S Department of Energy's Office of Electricity Delivery and Energy Reliability (OE) define Smart grid as “the digital technology that allows for two-way communication between the utility and its customers, and the sensing along the transmission lines.”[2]

The way that transforms the traditional power grid system to Smart Grid is the ability of the grid to give responses to events and conditions at instant time. The events may occur at the power generation, transmission, distribution, or consumption. But the Smart Grid should give responses within instant period of time. Figure 2-2 depicts the traditional power grid architecture.

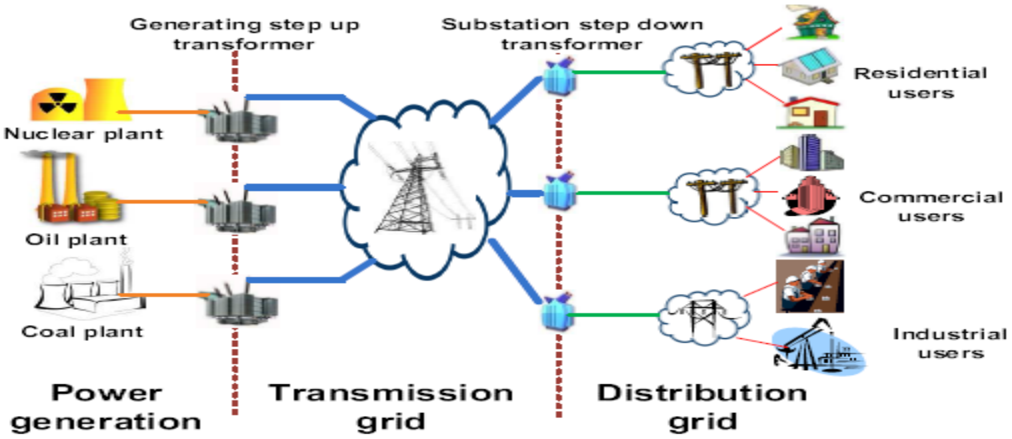


Figure 2-2: Traditional Power Grid architecture [21]

Fang, et al. [21] presented the difference between the traditional (current power grid) and Smart grid as shown in table 2 below.

Traditional Power Grid	**Smart Grid**
Electromechanical	Digital
One-Way Communication	Two-Way Communication
Centralized Generation	Distributed Generation
Hierarchical	Network
Few Sensors	Sensors Throughout
Blind	Self-monitoring
Manual Restoration	Self-Healing

[1] https://www.eia.gov/outlooks/ieo/world.cfm
[2] https://www.smartgrid.gov/the_smart_grid/smart_grid.html

Failures and Blackouts	Remote Check/Test
Limited Control	Pervasive Control
Few Customer Choices	Many Customer Choices

Table 2: Comparison between Traditional Power Grid and Smart Grid

Smart Grid Components

Smart Grid consists of all components from power generation till small home appliances that use electric power for different purposes. Hoang [22]identified five main Smart Grid components, which include:

i. **Intelligent appliances**: - Smart Appliances (Smart home appliances and other appliances) are becoming common in our daily life. Most of the industries which produce appliances are shifting their focus from traditional products to smart products. The benefits of these appliances are two folds. For example, you can save up to 25% energy consumptions by programming your appliances to reduce energy usage at peak load time [23].

ii. **Smart power meters (Smart Meter)** [22]: - is one of the components of Smart Grid which records automatically the energy consumption of the end users with in an interval of an hour or less to provide billing and other information to the power providers and for the end users. The Smart meter can read electric data such as Voltage and Frequency then up-to-date energy consumption details can be generated for the appropriate users. The generated data includes unique Id of the smart meter, timestamp of the data, electric consumption value and so on. As shown from figure 2-3 below Smart meter provides a two-way information flow between the meter and the central systems.

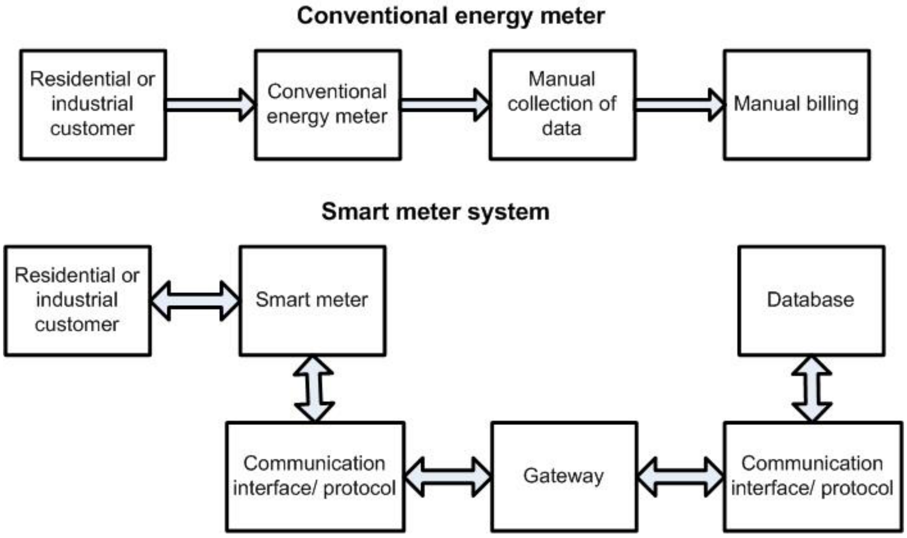

Conventional energy meter
Residential or industrial customer
Conventional energy meter
Manual collection of data
Manual billing
Smart meter system
Residential or industrial customer
Smart meter
Database
Communication interface/ protocol
Gateway
Communication interface/ protocol

Figure 2-3:Metering architectures of conventional energy meter and smart meter [24]

iii. **Smart distribution [25]: -** Power provides need to build several Distribution stations and transmission lines to transfer power from generator to consumers. The main aim of making distribution stations smart is to use the power efficiently and effectively by minimizing losses and adapting the capacity based on the consumption of power.

iv. **Smart Generation [24]: -** Generation is the various power generators used in the power generation system. This includes hydro-power, coal, nuclear, wind, and solar power generation system. The Smart Generation handles all these heterogeneous sources of power to cooperatively work the generation strategy without the interference of human being.

v. **Smart substations: - "**Smart substations monitor and control of critical and non-critical operational data such as power factor performance, breaker, transformer and battery status, security, etc." [26]

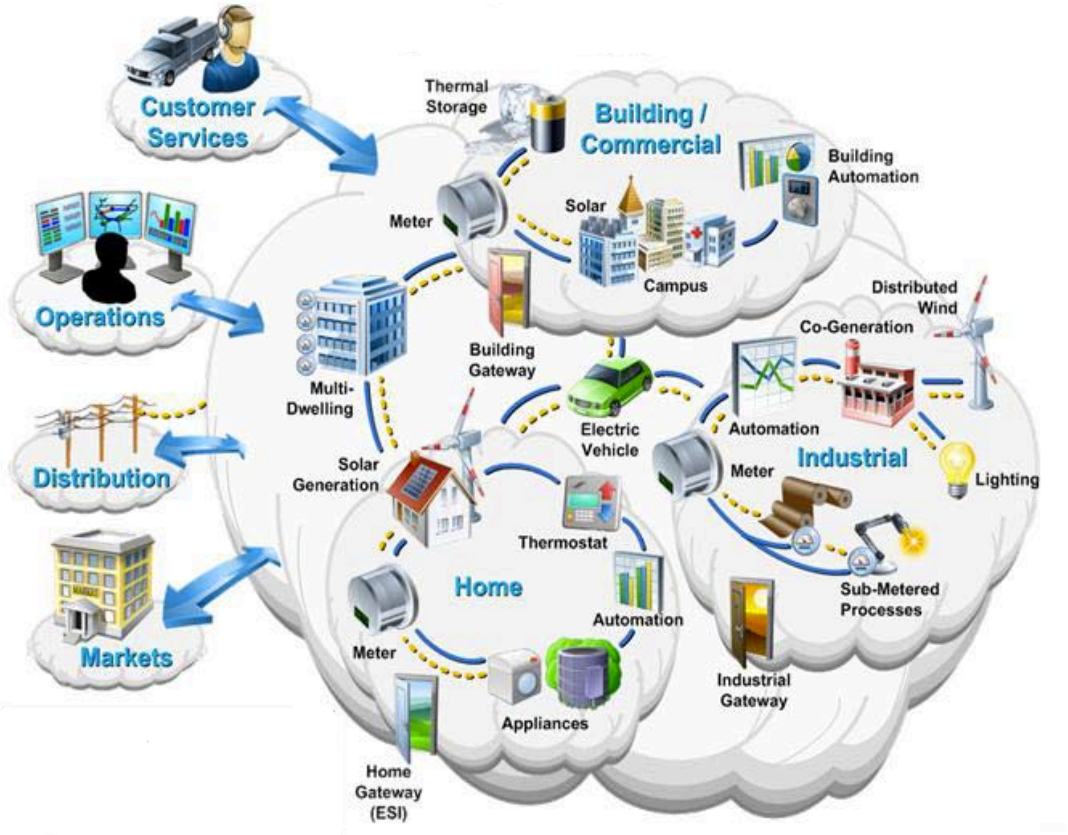


Figure 2-4:Smart Grid Infrastructure[3]

Smart grid Technologies: - Smart Grid is a collection of various technologies such as communication devices (wireless and wired), sensors, actuators, and software. According to [26] Smart Grid technologies can be grouped into five categories:

a. **Integrated Communications [22]**: - Smart grid uses almost use all wireless and wired communication technologies. The wireless communication technologies include wireless mesh network such as IEEE 802.11, 802.16, WiMax; cellular **c**ommunication system such as 3G, 4G, and GSM; satellite communication, MicroWave and wired communication technologies such as PLC, and fiber optics.

b. **Sensing and Measurement: -** As you can see from the above figure 2-4, Smart Grid is mainly made up of Sensing and measurements. Sensors are the main components of every components in Smart Grid to give automatic response for checking well-being and integrity of the grid [22].

c. Advanced Control Methods: - The advanced control methods are the devices, sensors and the algorithms used to control the power grid systems [26].

[3] http://iotap.mah.se/post-doc-radu-casian-mihailescu/

d. **Improved Interfaces and Decision Support: -** includes mobile applications, computer software, voice commands and simple user interfaces which is easy to understand and use for the power grid operators.

e. **Advanced Components:** - "are used to determine the electrical behaviour of the grid and can be applied in either standalone applications or connected together to create complex systems such as microgrids." [22]

2.3.2 Smart House

Smart house is one of the hot research area since the beginning of the new millennium. Smart home research survey which was conducted by Jiang, et al. [27] shows that numerous smart house research and projects were conducted in Europe, Asia, and USA. The projects were run by companies like CISCO, Microsoft, and Philip; and Universities and other research institutions. Since then many projects and researches that improve the energy efficiency, health care services, making smart appliances, improving security and surveillances, and improving the comfort of the life of the human being have been conducted.

Smart Home Energy[4] defined Smart home as

"*smart home, or smart house, is a home that incorporates advanced automation systems to provide the inhabitants with sophisticated monitoring and control over the building's functions. For example, a smart home may control lighting, temperature, multi-media, security, window and door operations, as well as many other functions.*"

Smart home is the interconnection of different devices and these devices have the capacity to share data between them. It also contains several sensors such as Gas leak sensor, Smoke Sensor, Wind and Rain Sensor, Door magnet sensor, Lighting switch, Body Sensor, and Air conditioner sensor.

Hoang [22] and Jiang, et al. [27] classified Smart homes into four application areas. These are: Energy management and Efficiency, Entertainment, Health care, and Security and Surveillance.

a) **Energy management and Efficiency: -** According to Norwegian Statistics Bureau energy consumption report of 2015 and 2014[5], the energy consumption of household was increased by 2% while the total energy consumption was increased only by 1.2%. Household shares the largest part of the world's energy consumption. The number of population growth and energy consumption have a direct relationship if we are using

[4] http://smarthomeenergy.co.uk/what-smart-home

[5] http://www.ssb.no/en/energibalanse

the tradition energy management system (hierarchical, and centrally controlled), i.e., as the number of population increases, the consumption of power also increases. In recent years, the use of smart appliances and connecting devices at home are increasing from time to time due to the emergence of IoT technologies. To ensure a sustainable and efficient use of energy system in homes, Information and communication technologies are playing a significant role. Reducing the cost of energy, and minimizing energy wastage of the homes by increasing the user's comfort are the main objective of energy management. Shifting from hierarchical and centrally controlled Grid system to Smart Grid and Smart meter technologies are helping to achieve these objectives.

b) **Entertainment:** - The invention of Internet and IoT enabled smart home revolutionized entertainment industry in fast-paced manner. It is possible to access any sound, image, or videos at any place. Smart home can be changed to home theatre, multimedia room, and distributed audio/video systems with a simple smart remote like smart watch by advanced user interface such as voice command, gestures, face recognition, scheduling task, etc[6].

c) **Health care**: - Smart home has improved and changed the traditional health care systems. Health care is one of the most sensitive services which needs accurate information. Smart home components such Appliances, sensors and Body area network devices support the health care system. For example, De Silva, et al. [28] designed a fridge that supports the health care system. One of the challenging things in this application area is that all devices and information are not available only in the smart house.

Even if so many promising results have been achieved in this application domain, there are still challenges that should be dealt with. The challenges are "usability, data privacy and security, integration and processing of diverse data streams, validation of clinical grade sensors, and the need for high quality evidence showing improved efficiency and cost-effectiveness." [29].

d) **Security and Surveillance:**- Smart houses have equipped and installed different devices and applications to control and follow the safety and security of its residents. Few of the systems and devices which are used for safety and security are:

- Movement sensors,

[6] https://www.youtube.com/watch?v=mEzSF29EBgI

- Video surveillance,
- Remote monitoring
- Alarming, etc

From these four smart home application areas, our focus is energy management and efficiency, and Security of Smart Home. The next section review Smart Home Energy Management Vulnerabilities, Attacks and Counter Measures.

2.3.3 Smart Home Energy Management Vulnerabilities, and Attacks

Beckers, et al. [30] proposed threat analysis of Smart Home Energy Management by following Microsoft Security Development Life Cycle. The threat analysis identifies vulnerabilities and possible attacks on Smart Home main components such as Smart Meter, Home Gateway, and SHEMS. They also proposed possible reasoning at each component. But the proposal didn't include possible countermeasures and also, they didn't implement their threat model.

Aloul, et al. [31] identified Smart Grid Vulnerabilities, Threats, and Solutions. They identified the infrastructure, attackers, attack types and possible solutions by reviewing different literatures. Both Beckers, et al. [30] and Aloul, et al. [31] didn't implemented their models.

2.4 IoT and Security Ontologies

As we have described in the above section, the infrastructure of Smart Grids and Smart houses consist of a bunch of Sensors, Communication technologies, heterogeneous environments, and heterogeneous devices.

In this section, we review Ontologies that are developed to handle different functions of IoT objects. After reviewing the ontologies, we compare them based on selected parameters to reuse some parts of the ontology in our work.

2.4.1 IoT Ontologies

2.4.1.1 Semantic Sensor Network (SSN) Ontology [32]

SSN is one of the widely used and customizable sensor ontology. SSN Ontology was designed and developed by W3C Semantic Sensor Network Incubator Group which consists of 39 members from 20 organizations. The members were from universities, small companies, multinational companies, and research institutions from USA, Germany, Australia, Germany, Ireland, Finland, Spain, China, and Korea. It was a one year project.

The focus of the project was designing and developing an ontology that describes sensors and observations. The description of the sensors includes measuring capabilities, operating conditions, survival conditions, sensor deployment, ways of sensing, and the output of the sensing. The final ontology consists of 41 classes (concepts) and 39 object properties organized in to modules as shown in the figure below. Some of the Concepts and Object properties are reused from DOLCE ultralite ontology (DUL)[7]. A single module of the ontology consists of one or more concepts.

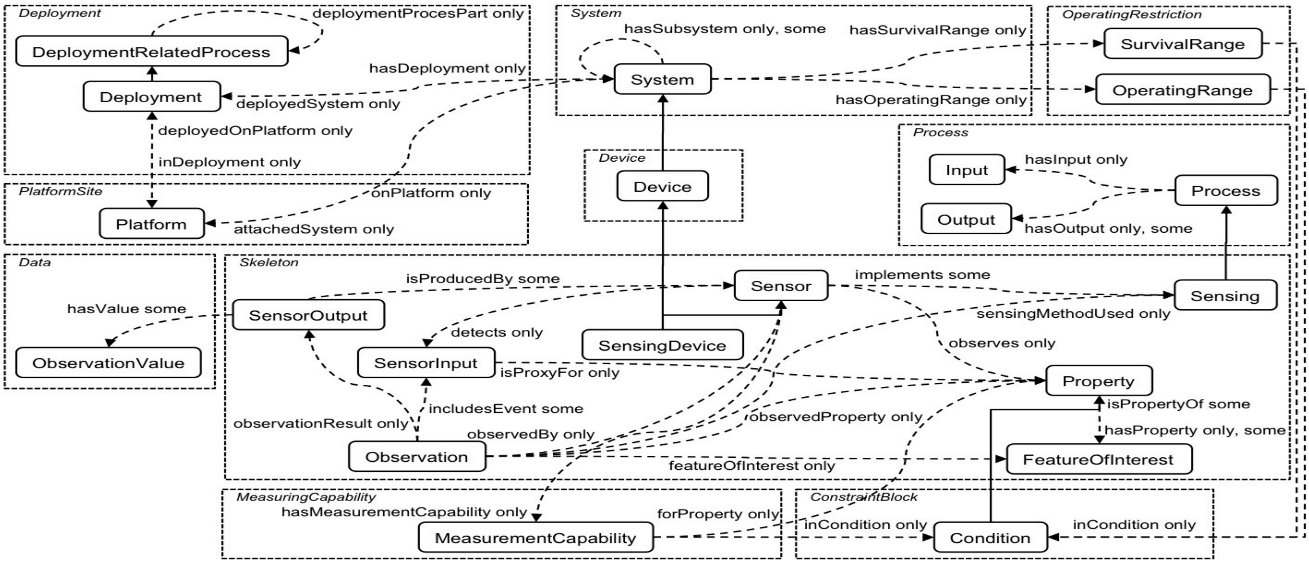


Figure 2-5:SSN Ontology [8]

This ontology didn't define data properties and didn't instantiate individuals. It shows only concepts and Object properties. Data Properties and individuals can be defined by the people who customize this ontology based on their needs.

W3C started an effort to standardize this ontology by publishing W3C First Public Working Draft on 31 May 2016[9]. The recent working draft is also launched on 04 May 2017[10]. They are a group of four people trying to solve the challenges of the previous version of SSN released on 2011. The group has identified different challenges and proposed the ideal solutions for standardizing the ontology. For example, one of the main challenges of SSN is its complexity; because one third of concepts and Object properties are inherited from DUL ontology. The group separated the SSN part that use DUL terms into the SSN alignment with DUL ontology.

[7] https://www.w3.org/2005/Incubator/ssn/wiki/DUL_ssn
[8] https://www.w3.org/2005/Incubator/ssn/XGR-ssn-20110628/
[9] https://www.w3.org/TR/2016/WD-vocab-ssn-20160531/
[10] https://www.w3.org/TR/vocab-ssn/

2.4.1.2 IoT-Lite

It is the instantiation of SSN Ontology [33]. The developers of this ontology believed that IoT ontologies should not be complex and should not increase possessing capacity. This ontology has Object, System and Services as the main classes as shown in figure 2-6 below. System has one sub class called Device. Device has SensingDevice, TagDevice and Actuating Device as its sub classes. In SSN Ontology Actuator, Location, and timing are not explicitly defined. But IoT- Lite Ontology defined these three concepts. In total the ontology consists of 18 classes and 13 object Properties. The group also proposed 10 rules for good and scalable semantic model design.

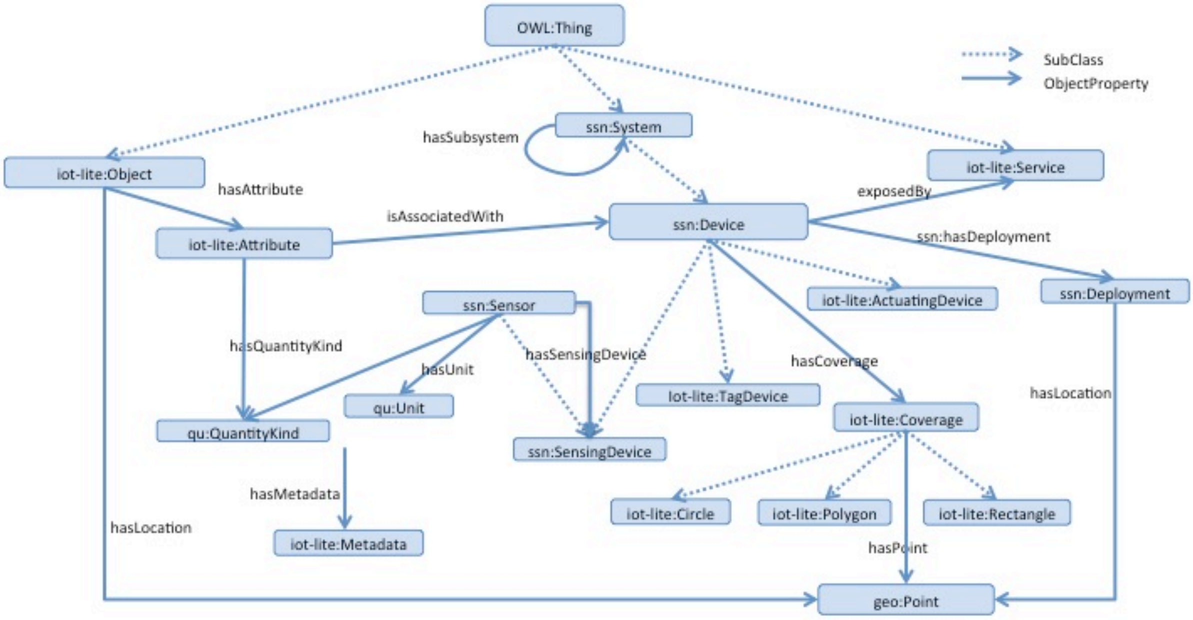


Figure 2-6: IoT-Lite Ontology [32]

2.4.1.3 SAREF [34]

SAREF ontology provides semantic interoperability between house appliances to save and use energy consumption efficiently. It is a standard reference ontology prepared by ETSI (European Telecommunications Standards Institute). It has more than 125 classes, 45 object properties, 12 data properties and instantiated few individuals[11]. At the beginning of 2017, SAREF ontology has been extended to SAREF4EE, Weather, and M2M(Industrial) domains by ETSI task force. The Energy domain ontology consists of 253 classes, 87 data properties, 97 object properties, and 173 individuals.

[11] http://ontology.tno.nl/saref/

2.4.1.4 Ontology-Based Smart Home Solution and Service Composition

Xu, et al. [35] proposed an ontology-based smart home architecture which contains four domain ontology system: Device Ontology, Environment Ontology, Function Ontology and Policy Ontology. Device Ontology defines the available device, properties and categorizes based on parameters such as processing capacity and energy capacity. Environment Ontology defines based on the season and temperature, and house owner's health condition. They stated that health and age of a person plays a significant role in arranging the energy of the home. Function ontology defines and labels devices according to the services they provide. For example, Devices that are using temperature control can be named as Temperature control devices. Policy ontology is a set of rules prepared to control the smart house. For example, "When the temperature is above 5 Celsius, Turnoff the heater."

2.4.1.5 Semantic information modelling for emerging applications in smart grid.

Zhou, et al. [36] model a Smart Grid knowledge base based on real-time consumption, infrastructure information, consumer behaviour, schedule information and natural condition. They represented their models by using one of the most widely used ontology language called OWL. Their ontology is categorized into six component ontologies. These are Electrical Equipment, Organization, Infrastructure, Weather, Spatial and Temporal Ontologies. While developing this Ontology, they reused standard and well developed ontologies from different sources to improve the interoperability of IoT in Smart Grid.

Ontologies	Open Access	Recommended	Scenario	Security and Privacy
SSN	✓	W3C	×	×
IoT-Lite	✓	W3C	×	×
SAREF	✓	ETSI	✓	×
Xu, et al. [35]	×	-	✓	×
Zhou, et al. [36]	×	-	✓	×

Table 3: Comparison of IoT Ontologies

We compared the ontologies based on four parameters. The parameters are:

Open Access: whether the ontology is availably freely or not.

Recommend by: There are thousands of ontologies available on the web; but the difficulty is finding the standard ontology. It is better to use Ontologies recommended by and Standardized by W3C and ESTI.

Scenario: The focus of the Ontology domain.

Security and Privacy: Does the Ontology supports security and privacy?

Our scenario is on Home Energy management system. As we can see from table 3 the best candidate Ontology that we can reuse to extend our work is SAREF ontology [34]. SAREF focuses on energy management, M2M communication, and Environment. We extend the energy management domain ontology.

2.4.2 Security Ontology

SANS institute defined Information Security as: "*Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption*." [12]

Information security products can be categorized into two: Traditional Information Security and Adaptive Information Security. Tradition Information Security have constant ways of handling threats; whereas Adaptive Information Security can monitor, learn, and adapt to vulnerabilities and threats of the environment and act based on the context[7, 37, 38]. As the context and threats changes, the security mechanism also changes. For example, changing the authentication mechanism according to the risk context, high risk or low risk.

The following sections review Security Ontologies. Some of the ontologies we reviewed are designed based on the adaptive concepts; whereas the rest are designed for traditional Security concepts.

2.4.2.1 An Ontology of Information Security

The aim of this ontology is to create common vocabulary related to general information security concepts [39]. "The ontology consists of 88 threat classes, 79 asset classes, 133 countermeasure classes and 34 relations between those classes."

Threat in information technology is an event that may expose your system at risk. There should be a way to handle these threats. This ontology has defined counter measure classes to mitigate risks. Asset is all resources such as data and all communication devices.

2.4.2.2 Ontology Based Approach for Network Security

This ontology has three top classes namely Network, Attack and Vulnerability. Based on parameter such as Time, Source port, Destination port, Source IP Address, Destination IP Address, Server, Attribute Source, and Name, Actor location, Scope of the network,

[12] https://www.sans.org/information-security/

Automation level, Goal of the network, and type of service predicts the chance of the attack to the system is either high or Low.

2.4.2.3 Ontology for attack detection [40]

This work mainly focuses on three areas. The first focus is ontological model of communication protocol. This component of the ontology describes HTTP Protocol attack, Request and response of HTTP protocol during malicious attacks. Second, Ontological Model of Attack, "This model captures the context of important web application attacks, various technologies used by the hackers, source and target of an attack, impact on the system components affected by the attack, vulnerabilities exploited by the attack and control in terms of policies for mitigating these attacks."

The other effort of this work is the proposal of best metrics for evaluating Security Ontologies. The identified metrics are Formal correctness/Accuracy/Validity of the model, Consistency and Soundness, Task orientation, Completeness and Conciseness (domain coverage), Expandability and Reusability, Clarity, Computational complexity, Integrity and Efficiency, System performance by using throughput and response time, Preciseness and Quality measure by using precision, recall and F-measure, Model expressiveness, Ontology expressiveness, Attack modeling formalism, Inference support, and Protocol layer for attack detection.

2.4.2.4 SecurOntology [41]

This ontology is defined to handle resources according to the organization hierarchy roles and permissions by using Access Control List method. To achieve this objective the developers defined 6 main classes and 8 main object Properties. The classes include: Resources, Owner, Roles, Permission, ResourceAndPermission, and ConsultInstance. The main power of this ontology is the rules defined by using the SWARL[13] for inferring and reasoning new knowledge.

2.4.2.5 Interoperability of Security-Enabled Internet of Things

Alam, et al. [42] developed an OWL-Ontology which consists of three domain ontologies: Sensor Ontology, Event Ontology and Access Control Ontology. The sensor Ontology describe not only the Sensors (devices), but also the data collected from the Sensors. The Event ontology describes faults occurred by the sensors and recommended actions to manage these faults. Access Control Ontology defines restriction for the resources. In this case, the resources are Sensors and Sensor data. By using Semantic Web Rule Language (SWRL) and

[13] https://www.w3.org/Submission/SWRL/

the Semantic Web Query–Enhanced Web Rule Language (SQWRL) rules, they managed to implement different access control policies for their scenarios.

2.4.2.6 Towards a Reference Ontology for Security in the Internet of Things

Mozzaquatro, et al. [43] reviewed a number of Generic Security Ontologies and proposed a reference ontology for IoT Security. They also tried to implement Adaptive Security concepts. Adaptive Security adjusts automatically the security parameters and constraints to mitigate security vulnerabilities and attacks. Adaptive security follows the control theory rule which is Monitor, Analyse, and Adapt based on the security model [37]. The ontology defines Assets, Vulnerabilities, Threats, Security Mechanism and Security Property. The main drawback of this ontology is that its security framework Assets, Vulnerabilities, Threats, Security Mechanism and Security Property is designed from the perspective of communication technologies and the architecture of the communication system.

2.4.2.7 Ontology-based Security Adaptation at Run-Time

This ontology fully defined the concept of Adaptive Security [44]. The ontology has Monitor, Analyser, Measure and Adapter based on the Context. The Context has desired and achieved security threshold. The adaptation happens either at run-time or start-up phase.

Table 4 below shows comparison of different IoT Security Ontologies:

Comparison	Generic	Adaptive	Open Access	Scenario	IoT
[42]	✓	×	×	-	×
[43]	✓	×	×	-	×
[37]	✓	×	×	-	×
[44]	×	×	×	-	
[45]	×	×	×	Railway	✓
[46]	✓	✓	✓	C2Net	✓
[40]	✓	✓	×	Smart space	×

Table 4:comparison of IoT Security Ontologies

The parameters used to compare the ontologies are:

Generic: Describe whether the ontology is general or not.

Adaptive Security: whether the ontology supports adaptive security concepts.

Open Access: The ontology is freely available on the web.

and **supporting IoT concepts**.

Chapter 3

3 Design and Scenario Description

3.1 Introduction

From the perspective of IoT Security and Privacy, we categorized Smart Grid in to six broad domains. As shown in the figure 3-1, the domains are Aggregators, Smart House, Critical Infrastructure, Distributed System Objects (DSO), Security and Privacy**.**

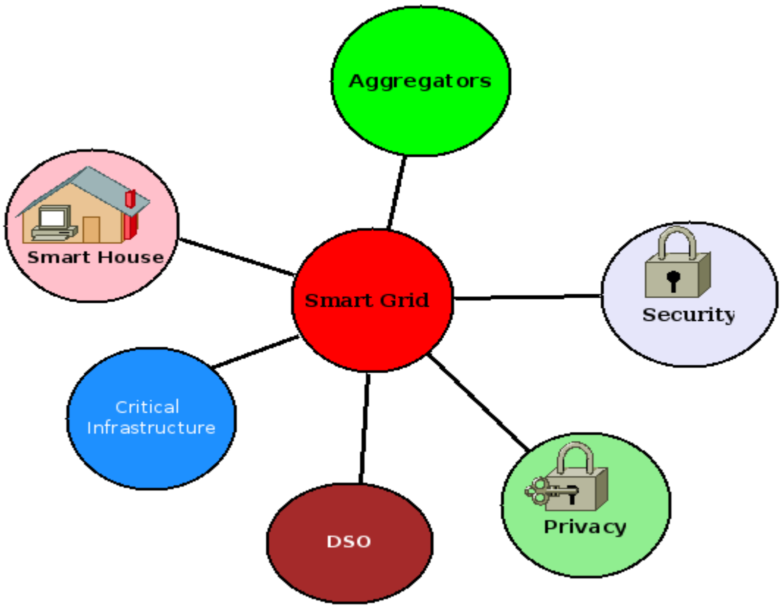


Figure 3-1: Smart Grid Architecture

From the above six domains of the Ontology, our focus is Smart House Energy Management System, and Security domains. Based on these two domains our scenario is described in the following section.

3.2 Scenario Description

This scenario description identified main components, threats, vulnerabilities, countermeasures and stakeholders of Smart Home Energy Management. The source of the information is Literature review.

Scenario name: Smart Home Energy Management Security (SHEMSec)

HEMS mainly consists the following Components [30]:

a) Application (SHEM)

b) Smart Meter

c) Smart Appliance

d) Home Gateway

e) Cryptographic Keystore
f) Personal Identifiable Information (PII)
g) Billing Data

3.2.1 Infrastructure and Service of SHEM [30]

a) The Home Energy Management System (HEMS)

HEMS is an application that is used to manage Smart Appliances, access billing data, and responds to Demand Side Management events. Energy Suppliers and other third parties communicate through HEMS.

External Dependency: Home Gateway or router provides the security and privacy of the communication infrastructure. Sometimes, Smart Meter is also used as a router.

Security Assumption: The Energy producers and consumers have access only to the user interface of energy management. They don't have permission for accessing or altering other functionalities.

Security Note: Consumers can access the interface of EMS by using mobile or other devices. They do not have the physical access of EMS.

Contains Assets: Cryptographic keys and Billing Data in real-time frequency.

b) Smart Meter

Smart is one of the components of Smart Grid which records automatically the energy consumption of the end users with in an interval of an hour or less to provide billing and other information to the power providers and for the end users. The Smart meter can read electric data such as Voltage and Frequency then up-to-date energy consumption details can be generated for the appropriate users. The generated data includes unique Id of the smart meter, timestamp of the data, electric consumption value and so on. If the measuremnet of Smart Meter is not accurate, it affects the billing, the energy forecast, demand side response, and all stake holders. Some Smart Meter is also used as a Gateway for Smart Home.

External dependency: If the Smart Meter is not a hybrid (functions as both Smart Meter and Home Gateway), it partially depends on Home Gateway to access EMS.

Security Assumption: The connection is stable and trustable through Home Gateway.

Security Notes: Technicians like Meter Point Operator (MPO) who install and configure devices like Smart Meter does not obtain any energy consumption data of the producers and consumers. Smart meter does not have permission to remotely shutdown energy.

Contains Assets: Billing Data, and Cryptographic keys

c) Home Gateway (HG)

Home Gateway is used as a communication channel for all devices and services of the internal Smart Home as well as external to the Smart Grid. For example, when SHEM wants to control Smart appliances, the request directly goes to Home Gateway. Then, HG authenticate the request, and gives permission for it.

External Dependency: The configuration of HG is done by the suppliers. They should ensure the availability and proper configuration of HG.

Security Assumptions: HG should support apply Authentication and Confidentiality. Configuration of addresses such as IP address and domain name should be configured properly.

Security Notes: producers and consumers should check the correctness of the receiving data. If there is any error, they should report to to MPO.

Contains Assets: Communication Keys for the Home Area Network.

d) Cryptographic keystores [30]

Every assets (HEMS, Smart Meter, Smart Appliances, and Home Gateway) has Cryptographic keystores.

External dependency: There are different protocols used for secret generation, key exchange and management. Each protocol has different level in securing the messages integrity and authenticity.

Security Assumptions: Key storage is only accessible internally by the device or the system.

e) Personal identifiable information: customer profile data, billing data

Personal Identifiable Information (PII) includes details of the consumer such as his name, address, personal number, Bank Account number, billing data, and Credentials.

External Dependency: Consumer billing data is the readings of Smart meter.

Security Assumptions: The reading of Smart Meter should be accurate.

Security notes: The cryptographic keystore should be protected from physically damage.

f) Define stakeholders [30]

The Home Energy Management stake holders include Domain Regulators, Legislators, Prosumer/consumer, Energy Supplier, 3rd Party Energy Supplier, Meter Point Operator, 3rd Party Service Supplier, etc.

3.2.2 Determine vulnerabilities [30]

1. HG vulnerabilities

The most common attack of HG is network attack. Since all devices and systems are connected to HG, it is vulnerable to attacks against these networks.

2. ***Smart Energy Meter vulnerabilities***

As of HG, Smart Energy Meter is vulnerable to network attack. It is connected to the smart home using WLAN or other communication technologies. Smart Meter´s should be tamper proof.

3. ***Home Energy management system vulnerabilities***

HEMS is an application accessible by a device like mobile and computer. It can be attacked by both Network and Software attacks.

3.2.3 Determine Threats to Home Energy Management System [30]

Spoofing: - is a Software attacker. It is a type of attack where unauthorized user access to a user's information which leads to information disclosure and denial of service. In this case, the attacker will alter, delete and controls the data and devices of the Smart home as his will.

Tampering: - is a Software attacker. In this scenario, the attacker can modify user policies, changing device parameters that might lead to burning and physically harming people around that area.

Repudiation: This attack type is Software attacker. An attacker can override non-repudiation mechanisms.

Information disclosure: - This attack type is Software attacker. The privacy of the user will be manipulated. Billing and other sensitive personal information might be exploited. All communication in Home Area Network will be publicised.

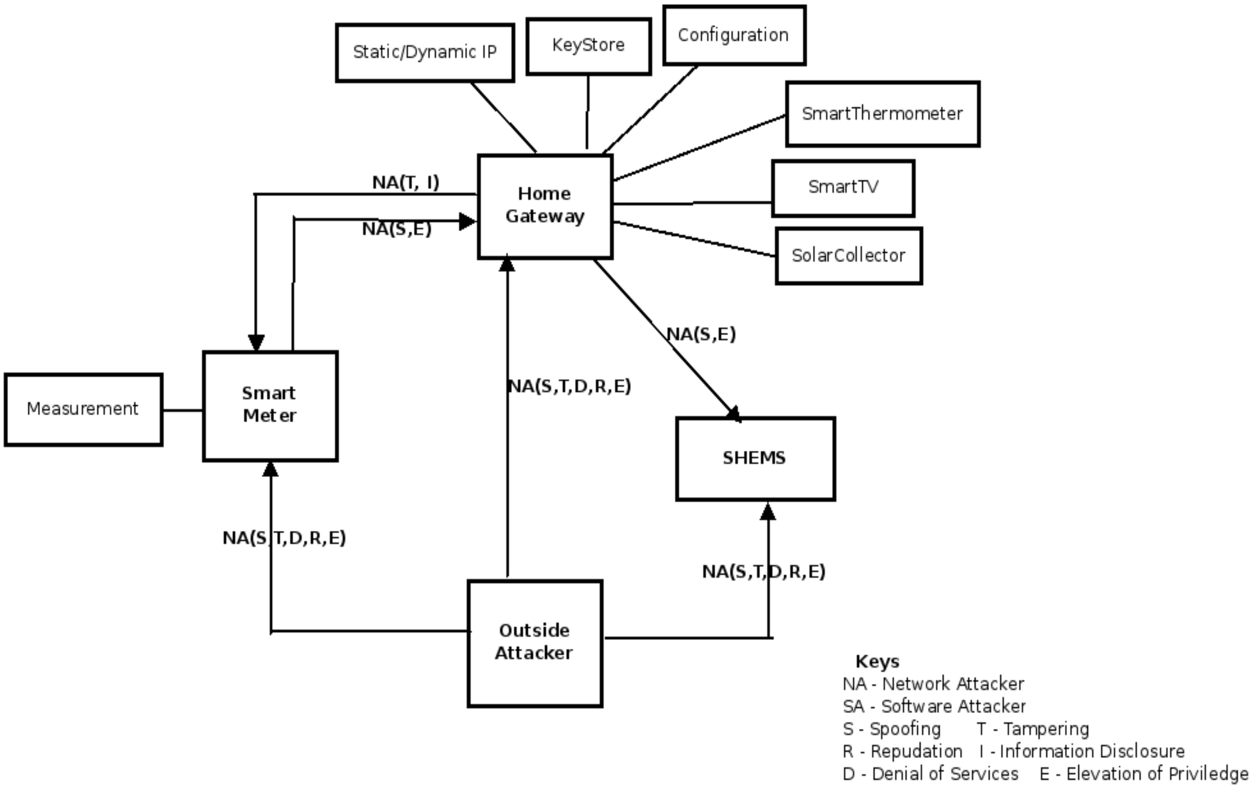


Figure 3-2: Threat from outside SH (Threat Model) [30]

Denial of service: This attack type is Software attacker. DoS lead to stopping all communication between Stake holders, denying access to EMS, and denying appliances and sensors control.

Elevation of privileges: This attack type is Software attacker. This attack type gives additional privilege for the user of the system. "The EMS supports third party plugins, which are allowed a sandboxed space in the EMS' functionality. If a malicious plugin is able to find a backdoor to the full EMS functionality, several assets could be compromised: Billing Data and customer profile data that identify the customer, cryptographic keys which allow proper authentication against the Energy Supplier, other third parties and the Smart Meter. The EMS controls the physical behaviour of Smart Appliances which might endanger the appliance itself or the well-being of persons inside the house." [30]

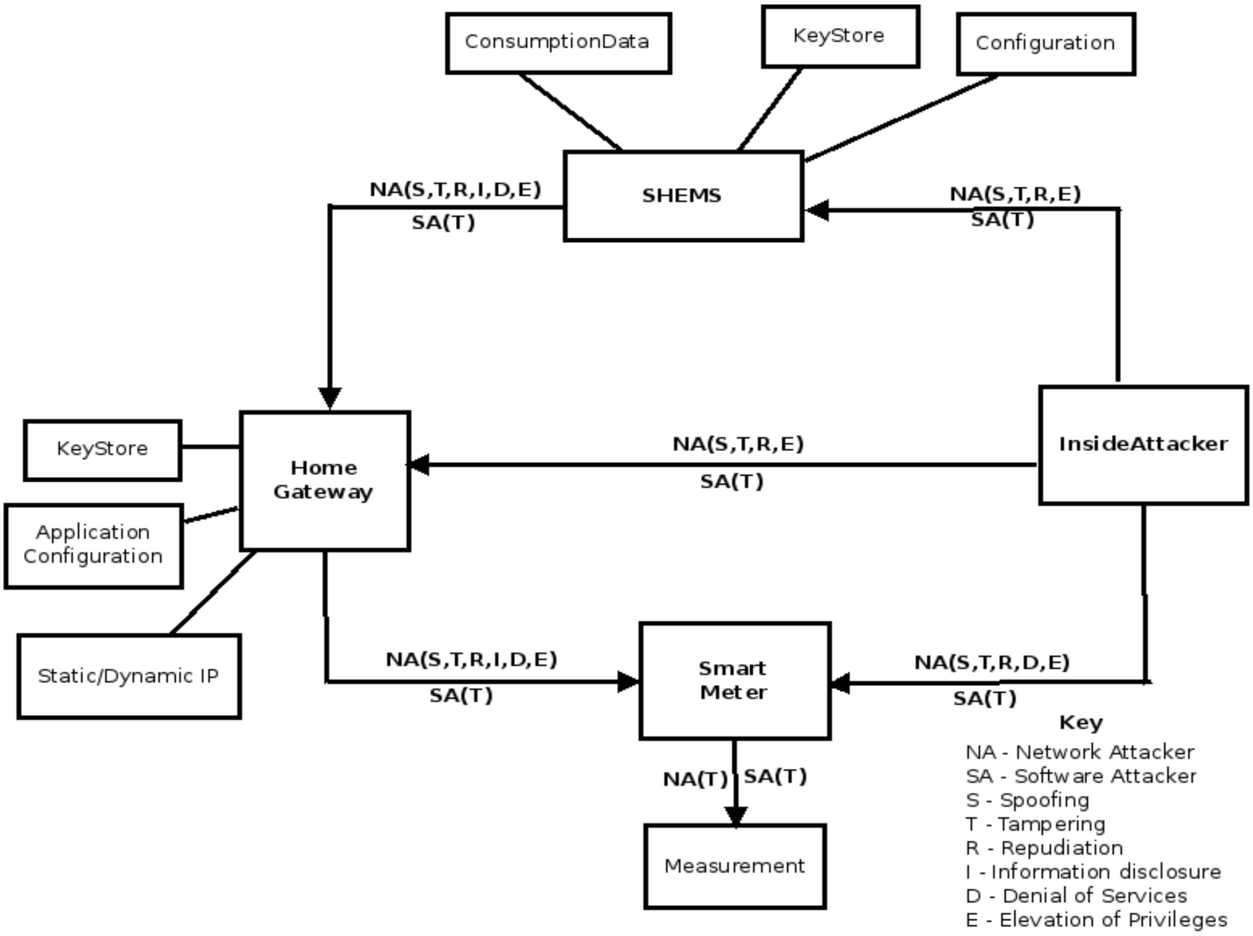


Figure 3-3: Threat from Inside (Threat Model 2) [30]

As we can see from figure 3-2 and 3-3, threats can be classified in to two: Inside Attacker and Outside Attacker. Inside attackers is a real user of a system. But he/she misuses his/her authorization to perform an attack on resources. Outside attackers do not have credential to use the system. They hack remotely the smart home energy resources such as billing data, smart appliance and sensors.

3.2.4 Counter Measures (Possible Solutions)

Security Mechanism or Counter Measures might be different for different types of security threats or attacks. Based on Literatures [30, 31, 38, 47-51], Microsoft[14], Cisco[15] and OWASP[16] security guide lines, the counter measures for the attacks described in 3.2.3 are:

Counter Measure for Spoofing: Spoofing mitigation mechanisms includes:

- Use Strong Authentication Mechanisms at the device, sensor, and application level.
- Encrypt passwords
- Use Secure communication protocols such as SSL, and HTTPs.

Counter Measure for Tampering: Tampering Can be mitigated by strong authorization, digital signature, hashing, secure communication links such as SSL and HTTPs, and use specific protocols designed for Tampering.

Counter measure for Information Disclosure: Information discloser can be mitigated by using strong authorization protocols, strong encryption protocols, encrypt passwords and other secrets, and using private-enhanced protocols.

Counter measure for Denial of service: The solution includes:

- Home gateway can filter address that can enter to the HAN by using Firewall and Access control mechanisms.
- Using trolling technique by controlling the data rate in to the HAN and out of the network.
- Using appropriate authorization for device, sensors and applications
- Using appropriate authorization for device, sensors and applications

Counter Measure for Elevation of privileges: Assigning the minimum role for the user. In addition to mitigating attacks at specific nodes, devices and systems, it is important to ensure the entire system is working correctly. The solutions that we have discussed above are not the only solution for these attacks. The attacks that might happen in SHEM can be mitigated by considering different parameter such as the environment, communication technologies, Software's used, etc. Each parameter might have specific security metrics to follow to mitigate the vulnerabilities of a System. The most common Security Mechanisms

[14] https://msdn.microsoft.com/en-us/library/ff648641.aspx

[15] http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

[16] https://www.owasp.org/index.php/Application_Threat_Modeling

are Access Control, Authorization, Authentication, Firewall, Encryptions, and mechanisms developed for specific technologies such as WiFi Security Mechanisms, Sensor Security Mechanisms, Firewall, antivirus, etc.

3.3 Ontology Design

The design of the ontology represents the relationship between basic components of the Smart Home Energy Managent components and Security components. The design follows risk analysis model which is recommended by ISO/IEC and National Institute of Standards and Technology(NIST). The top level classes include: ***Assets, Vulnerability, Threat, Security Property, Risk*** and ***Security Mechanisms.*** Figure 3-4 presents top-level classes of our security ontolog based on literatures [43, 45].

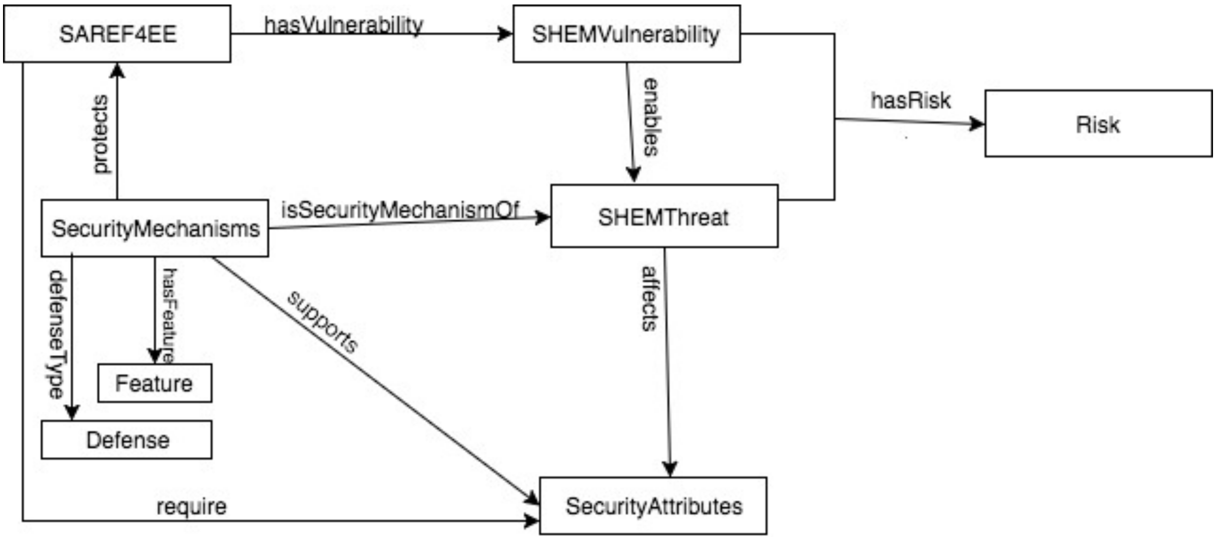


Figure 3-4: Security ontology top-level classes

Our Asset class is imported from SAREF Ontology extended for Home Energy Management. In this work Assets referes to all devices, sensors, communication technologies, and services of the Home Energy Management. The developers of SAREF ontology imported Geo and Time Ontology[17]. Geo and Time ontology describe location and temporal entity. SAREF ontology describes the energy management of Appliances. SAREF4EE is SAREF ontology extended for home energy management.

We extended SAREF4EE to develop Security ontology for Smart Home Energy Management.

[17] ttps://www.w3.org/TR/owl-time/

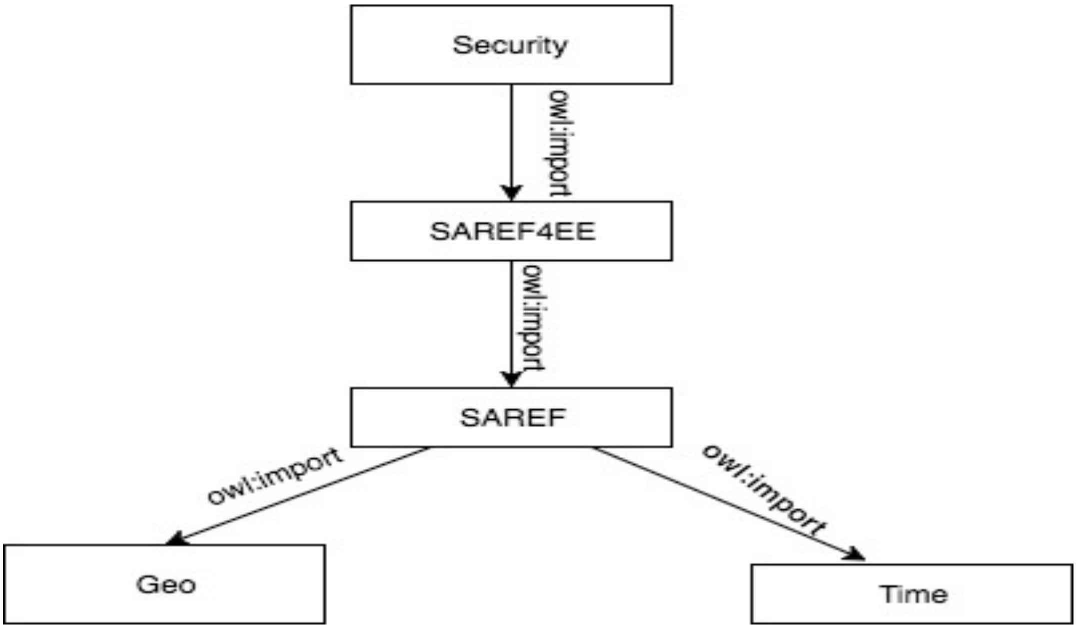


Figure 3-5: Structure of Imported ontologies

Assets have vulnerabilities. ***Vulnerability*** class describes potential flaws in the Smart Home Energy Environment.

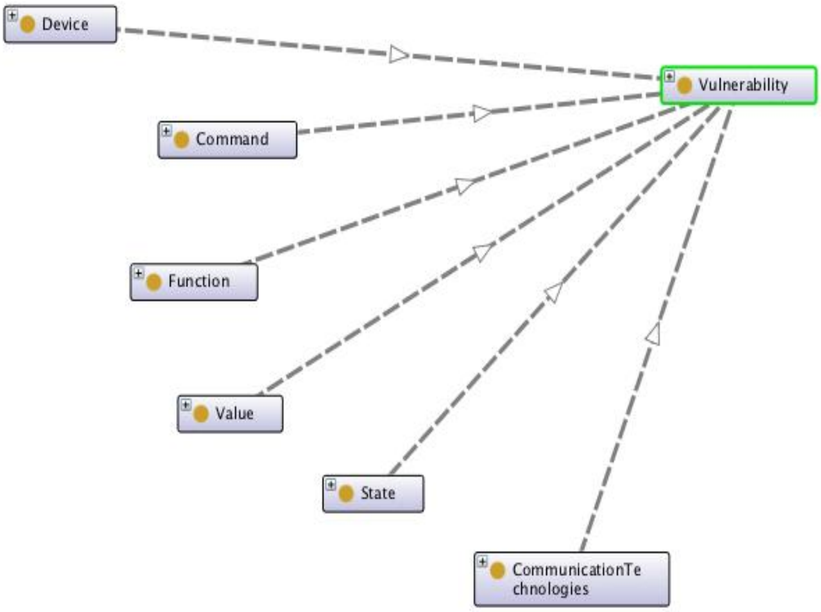


Figure 3-6: Asset(SAREF) Home Energy Management and Vulnerability (hasVulnerability) relationship

The flaws can occur either in software or hardware platforms. All devices, Sensors and Software's might have vulnerabilities.

Threat class consists of possible threats (attacks) that might happen in Smart Home Energy management. The threat identified in section 3.2.3 are: **Tampering, Denial of Service, Spoofing, Repudiation, Disclosure of Information, and Elevation of Privilege**. These threats affect security properties of Smart Home Energy Management System.

CounterMeasure class consists of algorithms, protocols or tools used for mitigating threats(attacks). This class has subclasses like ***Encryption, Firewall, Checksum, Hash, KeyManagement, Credentials,*** and ***TrustManagement.***

These protocols, tools, and algorithms are used by devices and applications. Some devices might not support the usual protocols and algorithms used by computer due to their processing capacity, memory and other factors. For example, Sensors nodes with limited processing capacities can use constrained device protocols instead of the usual protocols and algorithms. We also described protocols related to constrained devices.

Security Mechanism protocols, algorithms and tools ensure the security attributes of the smart home Energy management devices, sensors, and applications.

SecurityProperty class includes Availability, Integrity, confidentiality, Trust, and Non-Repudiation.

Risk level can be High, Low or Medium by multiplying likelihood and impact[18]

(Vulnerability and Threa

Smart home Energy Management has different users such as consumers, producers, technicians, 3rd party service provides, etc. By using Role-Base Access Control and Credential, we can ensure Confidentiality and Integrity.

Figure 3-8 Presents Role-Base Access Control Architecture for Smart Home Energy Management Application. The figure categorized the components in to User, Role, Credential, Command, Data Source.

Users: are any person/Device who uses the system.

Role: We categorized the role into Home Owner, AMI Operator, Producer, Service provider, etc. The Role gives permissions for specific group of users to access smart home data or devices. For example, Home owner can access billing data, turn on/off Appliances, and read sensor data. But AMI operator cannot access billing data.

[18] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

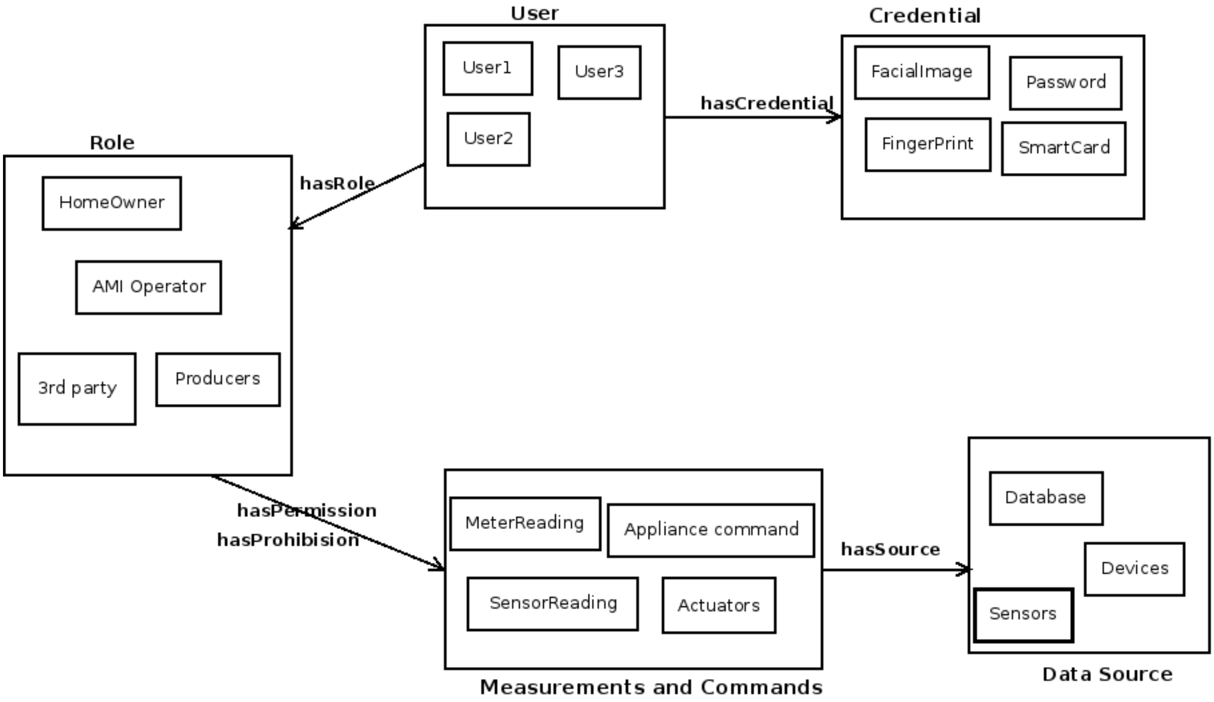


Figure 3-7: Smart Home Energy Management Access Control Architecture

Credentials: is a security mechanism that ensure confidentiality, and authenticity.

Measurement and Command: After the user is authenticated and based on role permission, she/she can access interface of the SHEMS (Command). The command includes reading billing data, turning off/On appliances and lights, pausing tasks and others.

Chapter Four

4 Implementation and Results

4.1 Introduction

For Developing our ontology we followed the guide proposed by Noy and McGuinness called Ontology Development 101 [52]. The guide illustrates seven steps that can be applied during ontology development process. It also describes a mechanism that can guide the developed to evaluate the ontology. The development process may need several iterations before producing the final ontology.

- **Step 1: Determine the domain and scope of the ontology:** The ontology should have precise domain and scope. For our work, the scope and the domain were fixed from the beginning. i.e., we focused on the smart House Energy Management Security domain.
- **Step 2: Consider reusing existing ontologies**: From the beginning reviewing available ontologies is beneficial. As we described in the previous chapter we have compared various ontologies and we have chosen to use SAREF ontology which is a reference Ontology for Smart Energy Management.
- **Step 3: Enumerate important terms in the ontology**: Before starting the ontology development, it is good to identify and write down all terminologies that is useful in the ontology. SAREF ontology which is extended for Home Energy Management consists of 253 classes, 87 data properties, 97 object properties, and 173 individuals. It has key terms such as Device, Command, Function, Property, State and Task. We also added Security Keywords such as ***Threat, CounterMeasures, SecurityAttributes, Spoofing, DenialOfService, InformationDisclosure, Encryption, SecureProtocol, Firewall, Integrity, Availability, Confidentiality,*** and much more.
- **Step 4: Define the classes and the class hierarchy:** As we have described in section 3.3, our ontology defined Infrastructure, Service, Attacks, Vulnerabilities, Threats, Counter Measures concepts and properties. The Infrastructure and Service of Home Energy Management concepts are imported from SAREF ontology. We can take these classes as an Assets of our system. Figure 4-1 shows the main classes of Assets or Systems of Home Energy Management imported from SAREF ontology.

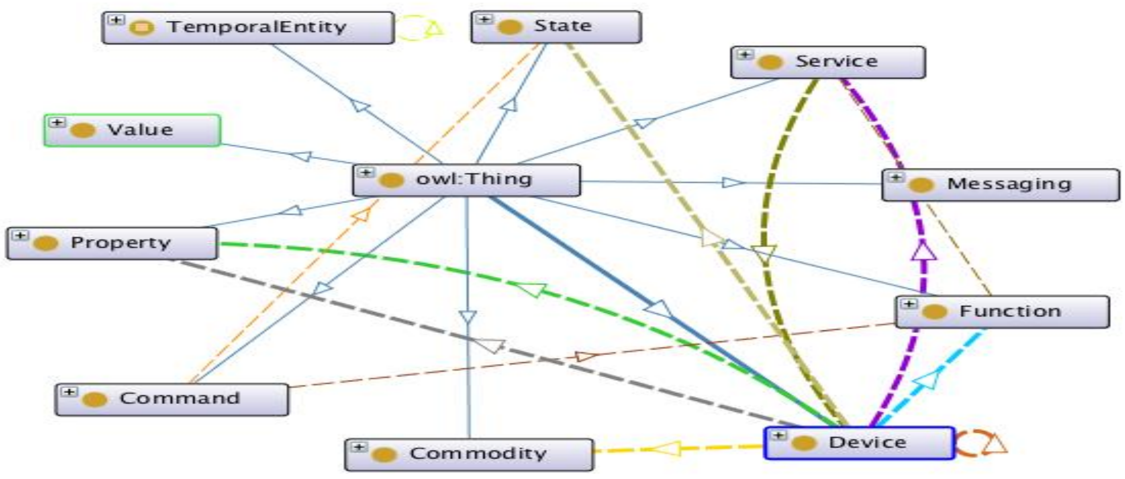


Figure 4-1: SAREF Ontology Main Classes

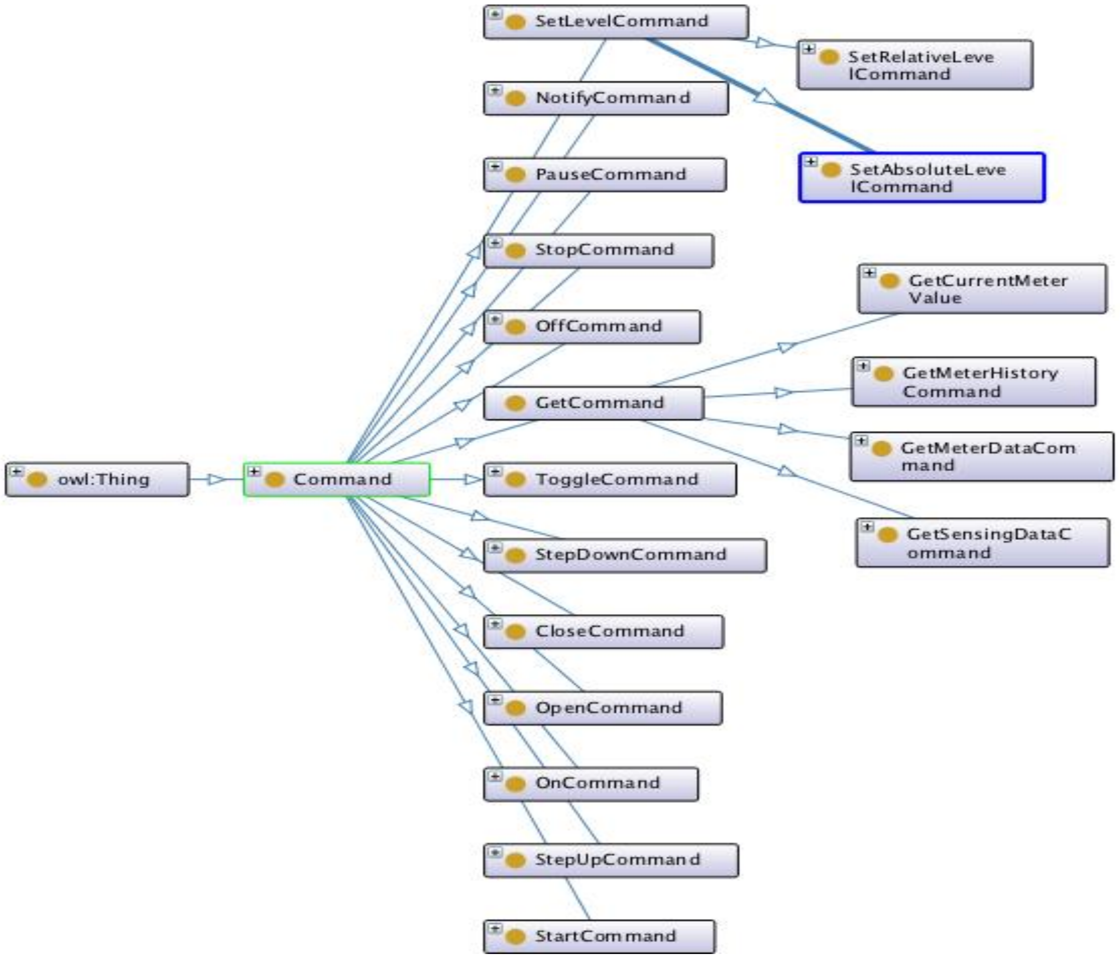


Figure 4-2: Command Class Hierarchy

One of the Infrastructure and Service class is Command class which is imported from SAREF ontology. It is used as an application interface(HEMS) to access the Smart meter readings, to Put On, Off Light and other Switch and Appliances, to close and open other devices. To access these commands, the user should be authenticated by using one of the Access control credentials.

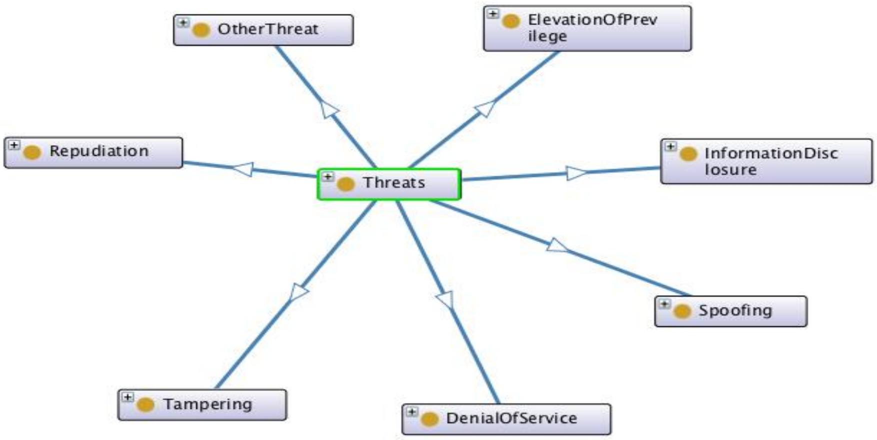


Figure 4-3: Threat class Hierarchy

Threat classes include all possible attacks that might happen in Home Energy Management Infrastructure and services. For example, Smart Meter might be attacked by Inside or outside attackers. The attack types include DoS, Spoofing, Repudiation, Information Disclosure, and other specific attacks related to infrastructure such as Sensor flooding and WiFi Attacks.

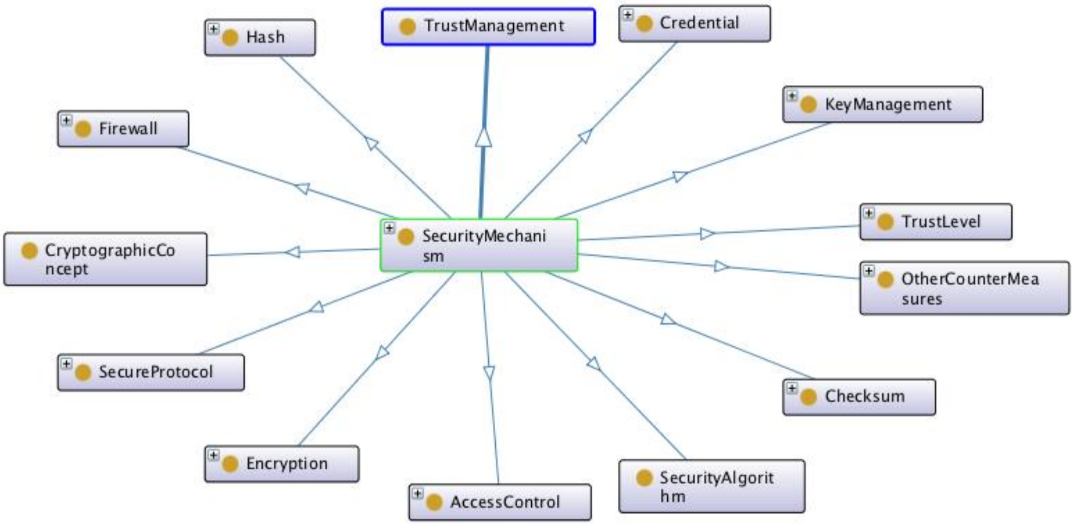


Figure 4-4: Security Mechanisms Class Hierarchy

SecurityMechanism class contains some of the Mechanisms used for mitigating attacks and vulnerabilities. Encryption, Firewall, Key Management, Secure Protocol, and others are used for ensuring availability, confidentiality, integrity, and accountability.

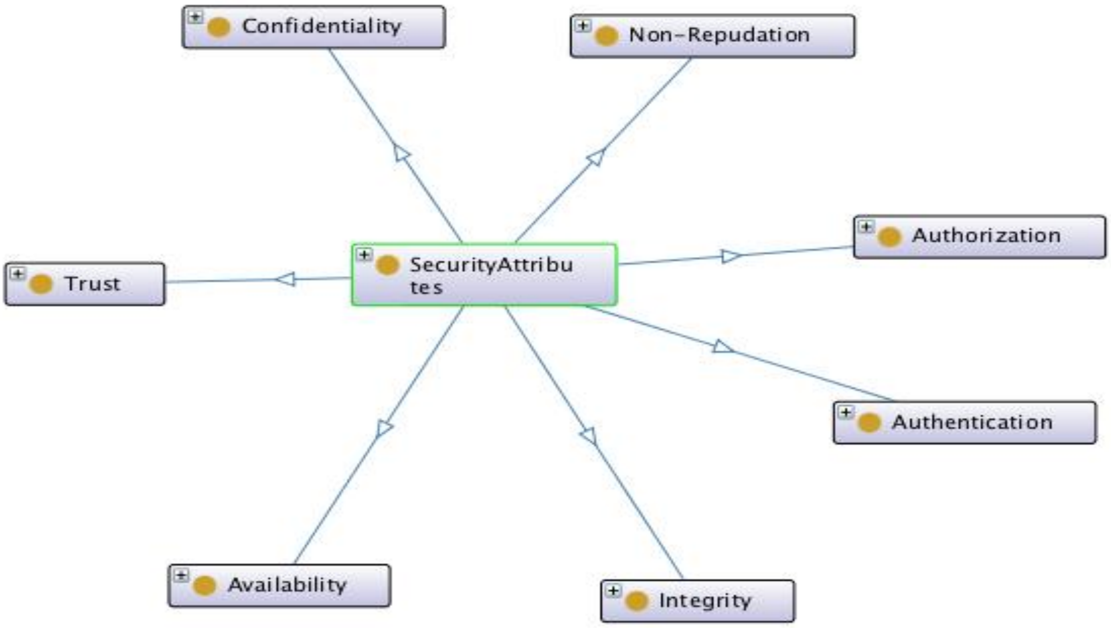
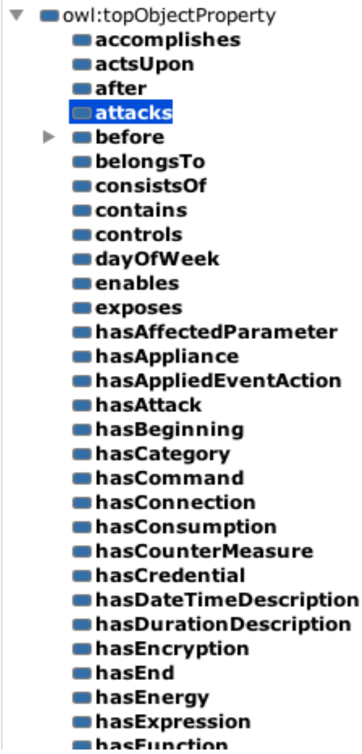


Figure 4-5: Security Attributes

SecurityMechanism class supports one or more Security attributes.

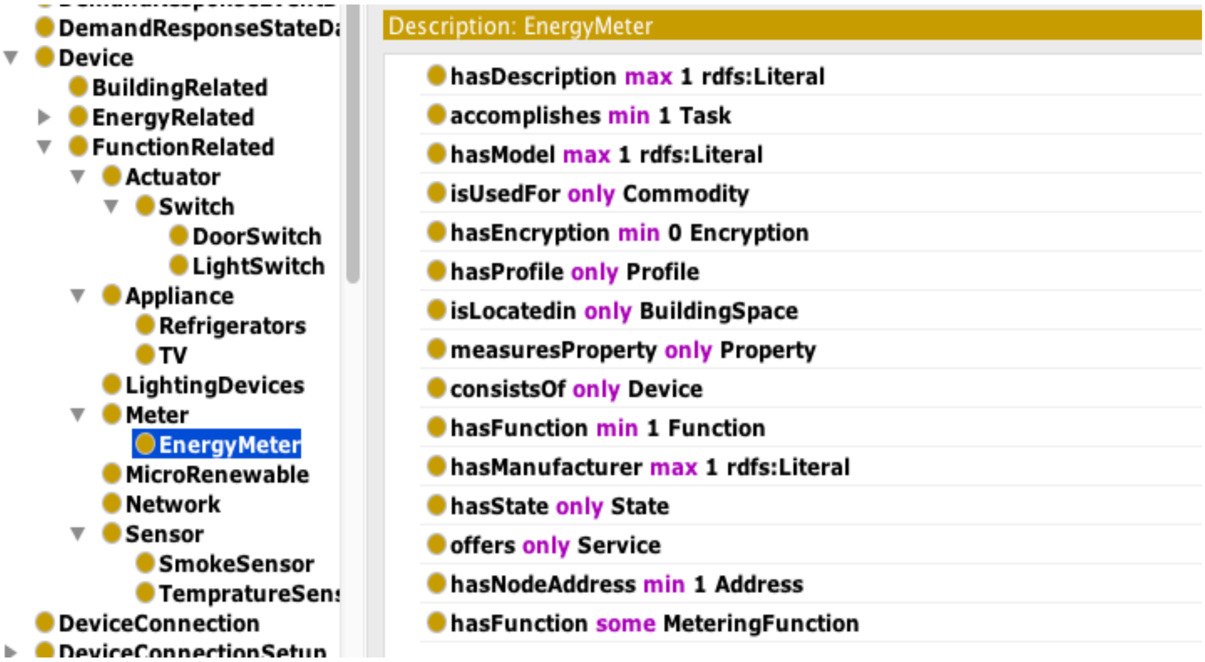
- **Step 5: Define the properties of classes and individuals**: Defining object and data properties is one of the most important parts of ontology development. While defining object and data properties, we can specify the domain and range of them.



```
▼ owl:topObjectProperty
    accomplishes
    actsUpon
    after
    attacks
  ▶ before
    belongsTo
    consistsOf
    contains
    controls
    dayOfWeek
    enables
    exposes
    hasAffectedParameter
    hasAppliance
    hasAppliedEventAction
    hasAttack
    hasBeginning
    hasCategory
    hasCommand
    hasConnection
    hasConsumption
    hasCounterMeasure
    hasCredential
    hasDateTimeDescription
    hasDurationDescription
    hasEncryption
    hasEnd
    hasEnergy
    hasExpression
    hasFunction
```

Figure 4-6: Object property

- **Step 6: Define the facets of the properties**: Inverse property, cardinality (number of values), and supported values are some of the facets of properties. Figure 4-6 presents the number of values(cardinality) of object and Data properties of Energy Meter.



```
  DemandResponseStateD
▼ Device
    BuildingRelated
  ▶ EnergyRelated
  ▼ FunctionRelated
    ▼ Actuator
      ▼ Switch
          DoorSwitch
          LightSwitch
    ▼ Appliance
        Refrigerators
        TV
      LightingDevices
    ▼ Meter
        EnergyMeter
      MicroRenewable
      Network
    ▼ Sensor
        SmokeSensor
        TempratureSens
  DeviceConnection
▶ DeviceConnectionSetup
```

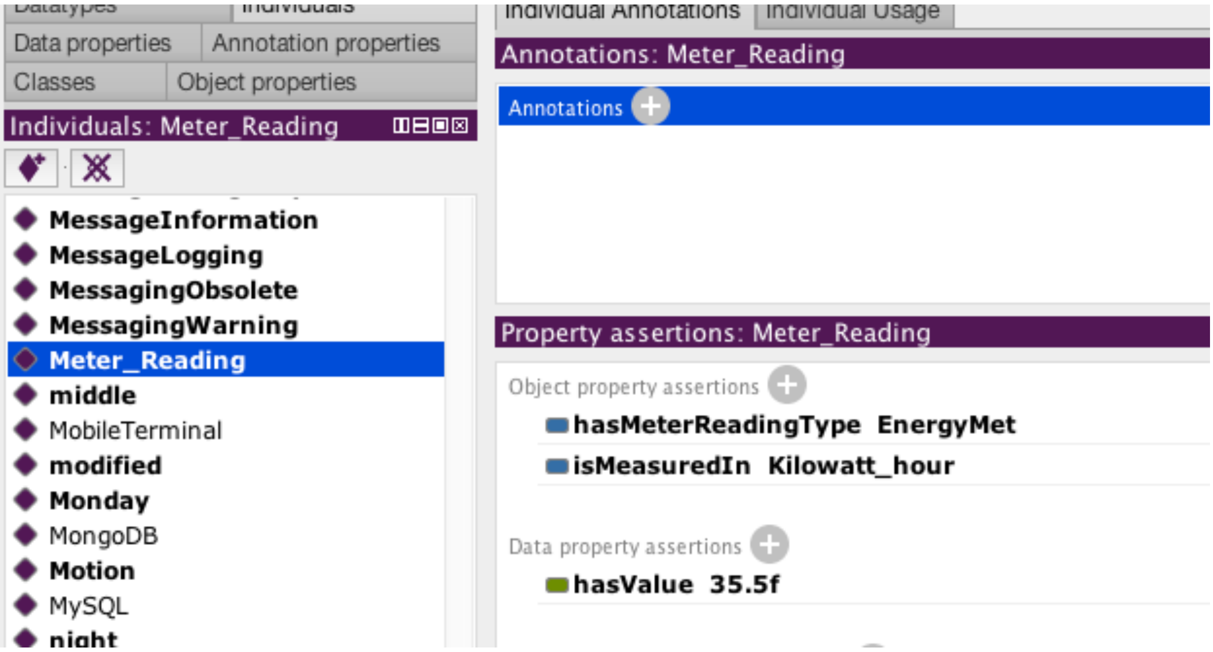
Description: EnergyMeter

- hasDescription max 1 rdfs:Literal
- accomplishes min 1 Task
- hasModel max 1 rdfs:Literal
- isUsedFor only Commodity
- hasEncryption min 0 Encryption
- hasProfile only Profile
- isLocatedin only BuildingSpace
- measuresProperty only Property
- consistsOf only Device
- hasFunction min 1 Function
- hasManufacturer max 1 rdfs:Literal
- hasState only State
- offers only Service
- hasNodeAddress min 1 Address
- hasFunction some MeteringFunction

Figure 4-7: Properties of Energy Meter

- **Step 7: Create instances (individuals) individuals are the lowest granularities of**

the ontology. Individuals have inherited properties from classes that they belong to.



MessageInformation
MessageLogging
MessagingObsolete
MessagingWarning
Meter_Reading
middle
MobileTerminal
modified
Monday
MongoDB
Motion
MySQL
night

hasMeterReadingType EnergyMet
isMeasuredIn Kilowatt_hour

hasValue 35.5f

Figure 4-8: Sample Individual

As we can see from figure 4-7, Individual named ***Meter_Reading*** has an instance value meter reading type **EnergyMet**(energy meter) which is measured by kilowatt per hour and has measurement value of 35.5.

4.2 Evaluation of the Ontology

The ontology can be evaluated by creating rules, inferring the knowledge and running Queries. OWL uses SWRL rule and SPARQL query to execute inference results from the developed ontologies. We create rules and run queries based on our Scenario.

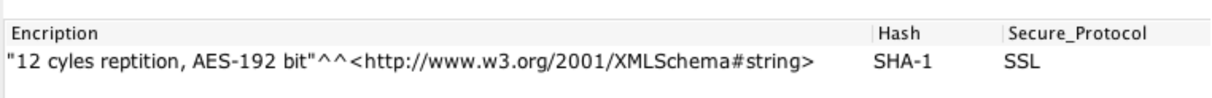
Query 1: Does the Smart Meter has Mitigation technique for Spoofing?

Spoofing can be mitigated by strong authentication, using Hash Function for storing keystore, password, other data and using protected Protocols such as SSL.

Query 1:

```
SELECT ?Encription ?Hash ?Secure_Protocol
          WHERE { :Smart_Electric_Meter :hasEncryption ?En.
                    ?En :hasValue ?Encription.
                :Smart_Electric_Meter :hasHash ?Hash.
              :Smart_Electric_Meter :hasSecureProtocol ?Secure_Protocol.}
```

Result 1:



Encription	Hash	Secure_Protocol
"12 cyles reptition, AES-192 bit"^^<http://www.w3.org/2001/XMLSchema#string>	SHA-1	SSL

While we execute the above query, as shown from the result, the device has a capacity of using AES Encryption algorithm, supports SHA-1 hash function and use SSL protocol. The probability of spoofing attack is low.

Rule 1: Categorize devices in the SHEMS as High, Medium, or Low Spoofing attack probabilities.

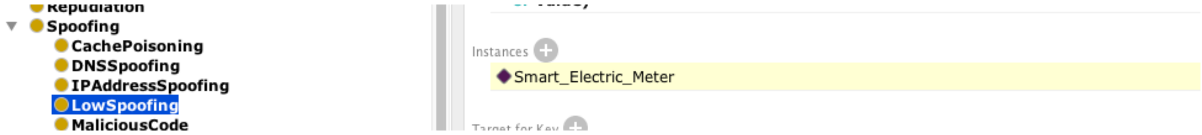
Let d be Device, e be Encryption, h be Hash Function, s be Secure protocol

If a device supports encryption algorithm or protocol, Hash Function and Secure protocol the chance of spoofing attack is very low. Rule 1 checks whether the device supports Hash Function, Encryption, Secure Protocol, Encryption key bit size. If the Encryption key bits size is between 128 and 512, it categorize the device as less likely to be affected by Spoofing.

Rule 1:

```
Device(?d)^ hasHash(?d, ?h)^ hasSecureProtocol(?d, ?p)^ hasEncryption(?d, ?e)^
hasBitSize(?e, ?b)^swrlb:greaterThan(?b, "128"^^xsd:int)^ swrlb:lessThan(?b, "512"^^xsd:int) ->
LowSpoofing(?d)
```

Result:



After running the reasoner, Smart_Electric_Meter is categorized as LowSpoofing device. The reason is that the device satisfies all the above requirements . The parameters of the device used are:

Smart_Electric_Meter	
hasHash	SHA-1
hasSecureProtocol	SSL
hasEncryption	AES
hasBitSize	192

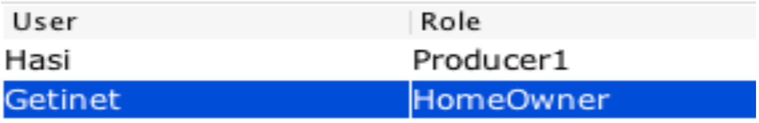
Table 5: Smart_Electric_Meter Parameters

Query 2: Display all users with their Roles

SPARQL Query:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX : <http://www.sgems.get/energys#>
SELECT ?User ?Role
        WHERE { ?User rdf:type :User.
                ?User :hasRole ?Role.}
```

Result:



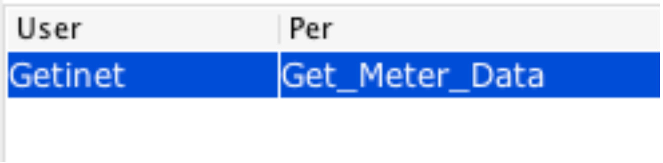
User	Role
Hasi	Producer1
Getinet	HomeOwner

As we can see from the result, User Hasi has a role as Producer1; whereas Getinet has **HomeOwner** role.

Query 3: Display all users' who has permission to read Smart Meter data with Role **HomeOwner.**

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX : <http://www.sgems.get/energys#>
SELECT Distinct ?User ?Per
        WHERE {?User rdf:type :User.
                ?User :hasRole :HomeOwner.
                ?Role :rolehasReadMeterDataPermission ?Per.}
```

Result:



User	Per
Getinet	Get_Meter_Data

The result shows, user Getinet has permission to read smart meter

Chapter 5

5 Conclusion and Future Work

5.1 Conclusion

In the previous chapters, we reviewed the technologies in the smart Grid domain, and explained the proposed IoT security ontology, and described the implementation and the evaluation of the prototype built based on the proposed architecture. In this chapter, we summarize and conclude the main contribution of this thesis. Further, we also present the future research directions based on this work.

5.2 Conclusion

This research work proposed, developed and evaluated IoT Security ontology for smart home energy management. The Ontology description includes infrastructure, attacks, vulnerabilities and countermeasures of main components of SHEMS such as Smart Meter, Smart Appliance, Home Gateway, and Billing data. The ontology is built as an extension to SAREF energy management Ontology by adding Security features. We have two main reasons for selecting SAREF ontology for our work. First, SAREF is standardized by ETSI. Second, it is designed for energy management and efficiency. We checked the correctness of our Ontology by running SWRL rule and SPARQL query languages.

5.3 Discussion

This section discusses the summary of the achievements accomplished during the research work in the development of the Ontology. A detailed discussion advances different aspects as follows:

5.3.1 Objectives Fulfillment

The analysis, development and evaluation work of our ontology succeeded in the fulfillment of the initial objectives of this research which is defined in the first chapter. The first objective was to analyze the requirements of IoT security in Smart Energy Management System. Accordingly, we analyzed the main infrastructure, attacks and counter measures of Smart Home Energy management system from different scientific papers. The second object was to review available ontologies related to IoT and Security. We reviewed Standardized Ontologies and Other Ontologies published in scientific journals. After we reviewed the ontologies, we compared them by using selected parameters. Based on our comparison result, we selected the best ontology for our goal and extended it in our work.

The other objective was to develop the ontology. The development of the ontology was done by following Ontology development guidelines. The ontology integrates the smart home energy management system and IoT security. We evaluated our ontology by running different security issue queries.

5.3.2 Contribution

The thesis work contributes to the practical knowledge that enables the precise integration of Smart Energy and IoT-based applications domains, as well as the development and validation of the ontology. The significance of our ontology includes:

(1) Specific ontology for SHEM IoT-based application that can assist in assessing and predicting the vulnerabilities, possible attacks and possible countermeasures.

(2) The users of the system have categorized according to their roles as consumers, producers, 3rd party users, etc.

(3) The Ontology gives specific focus for components in the SHEM domain.

5.4 Future Work

It would very interesting to apply our ontology to the multi metrics approach being developed in the IoTSec project.

6 Reference

[1] S. E. Bibri, *The Shaping of Ambient Intelligence and the Internet of Things*. Springer, 2015.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems,* vol. 29, no. 7, pp. 1645-1660, 2013.

[3] D. Evans. (2011, May 04,). *The Internet of Things*. Available: [Online]. Available: http://www.cisco.com/web/about/ac79/

docs/innov/IoT_IBSG_0411FINAL.pdf.

[4] I. Technology. (March 17, 2015). *Smart Grid Sensors Market Expected to Hit $350 Million in 2021*. Available: [Online]. Available: http://news.ihsmarkit.com/press-release/technology/smart-grid-sensors-market-expected-hit-350-million-2021-ihs-says

[5] marketsandmarkets.com, "Smart Grid Security Market by Solution, Service, Deployment Mode (Cloud, On-premises), Subsystem (SCADA/ICS, AMI, Demand Response, and Home Energy Management), Security Type (Endpoint, Network, Application, Database), and Region - Global Forecast to 2021," February 2017, Available: [Online]. Available: http://www.marketsandmarkets.com/Market-Reports/smart-grid-security-market-112912959.html, Accessed on: May 05, 2017.

[6] P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*. River Publishers, 2013.

[7] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 269-275: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[8] S. P. NIST, "800-12: An Introduction to Computer Security–The NIST Handbook," ed: October, 1995.

[9] T. Berners-Lee, Hendler, J., and Lassila, O., "The semantic web," *Scientific american,,* vol. 284, no. 5, pp. 28-37, 2001.

[10] I. Horrocks and P. F. Patel-Schneider, "KR and reasoning on the semantic web: OWL," in *Handbook of Semantic Web Technologies*: Springer, 2011, pp. 365-398.

[11] P. Hitzler, M. Krotzsch, and S. Rudolph, *Foundations of semantic web technologies*. CRC Press, 2009.

[12] D. Allemang, and Hendler, J., "Semantic web for the working ontologist: effective modeling in RDFS and OWL," *Elsevier,* 2011.

[13] B. Chandrasekaran, J. R. Josephson, and V. R. Benjamins, "What are ontologies, and why do we need them?," *IEEE Intelligent Systems and their applications,* vol. 14, no. 1, pp. 20-26, 1999.

[14] M. A. Musen, "The Protégé project: A look back and a look forward," *AI matters,* vol. 1, no. 4, pp. 4-12, 2015.

[15] T. Tudorache, J. Vendetti, and N. F. Noy, "Web-Protégé–Protégé going Web," *Stanford Center for Biomedical Informatics Research, Stanford University, CA, US,* 2008.

[16] P. Haase *et al.*, "The neon ontology engineering toolkit," *WWW,* 2008.

[17] A. Kalyanpur, B. Parsia, E. Sirin, B. C. Grau, and J. Hendler, "Swoop: A web ontology editing browser," *Web Semantics: Science, Services and Agents on the World Wide Web,* vol. 4, no. 2, pp. 144-153, 2006.

[18] R. Liepinš, M. Grasmanis, and U. Bojars, "OWLGrEd ontology visualizer," in *Proceedings of the 2014 International Conference on Developers-Volume 1268*, 2014, pp. 37-42: CEUR-WS. org.

[19] M. Hepp, D. Bachlechner, and K. Siorpaes, "OntoWiki: community-driven ontology engineering and ontology usage based on Wikis," in *Proceedings of the 2006 international symposium on Wikis*, 2006, pp. 143-144: ACM.

[20] C. Ghidini, M. Rospocher, and L. Serafini, "Moki: a wiki-based conceptual modeling tool," in *Proceedings of the 2010 International Conference on Posters & Demonstrations Track-Volume 658*, 2010, pp. 77-80: CEUR-WS. org.

[21] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE communications surveys & tutorials,* vol. 14, no. 4, pp. 944-980, 2012.

[22] B. Hoang, "Smart Grids," *IEEE Emerging Technologies Portal.[Online]* http://www/. *ieee. org/portal/site/emergingtech/techindex. jsp,* 2008.

[23] H. Farhangi, "The path of the smart grid," *IEEE power and energy magazine,* vol. 8, no. 1, 2010.

[24] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and sustainable energy reviews,* vol. 15, no. 6, pp. 2736-2742, 2011.

[25] J. Zheng, D. W. Gao, and L. Lin, "Smart meters in smart grid: An overview," in *Green Technologies Conference, 2013 IEEE*, 2013, pp. 57-64: IEEE.

[26] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Communications Magazine,* vol. 49, no. 4, 2011.

[27] L. Jiang, D.-Y. Liu, and B. Yang, "Smart home research," in *Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on*, 2004, vol. 2, pp. 659-663: IEEE.

[28] L. C. De Silva, C. Morikawa, and I. M. Petra, "State of the art of smart homes," *Engineering Applications of Artificial Intelligence,* vol. 25, no. 7, pp. 1313-1321, 2012.

[29] Y. B. D. Trinugroho, F. Reichert, and R. W. Fensli, "A SOA-based health service platform in smart home environment," in *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*, 2011, pp. 201-204: IEEE.

[30] K. Beckers, S. Faßbender, M. Heisel, and S. Suppan, "A threat analysis methodology for smart home scenarios," in *International Workshop on Smart Grid Security*, 2014, pp. 94-124: Springer.

[31] F. Aloul, A. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart grid security: Threats, vulnerabilities and solutions," *International Journal of Smart Grid and Clean Energy,* vol. 1, no. 1, pp. 1-6, 2012.

[32] M. Compton *et al.*, "The SSN ontology of the W3C semantic sensor network incubator group," *Web semantics: science, services and agents on the World Wide Web,* vol. 17, pp. 25-32, 2012.

[33] M. Bermudez-Edo, T. Elsaleh, P. Barnaghi, and K. Taylor, "IoT-Lite: A Lightweight Semantic Model for the Internet of Things," in *Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016 Intl IEEE Conferences*, 2016, pp. 90-97: IEEE.

[34] L. Daniele, F. den Hartog, and J. Roes, "Created in close interaction with the industry: the smart appliances reference (SAREF) ontology," in *International Workshop Formal Ontologies Meet Industries*, 2015, pp. 100-112: Springer.

[35] J. Xu *et al.*, "Ontology-Based Smart Home Solution and Service Composition," in *ICESS*, 2009, pp. 297-304.

[36] Q. Zhou, S. Natarajan, Y. Simmhan, and V. Prasanna, "Semantic information modeling for emerging applications in smart grid," in *Information Technology: New Generations (ITNG), 2012 Ninth International Conference on*, 2012, pp. 775-782: IEEE.

[37] H. Abie, "Adaptive security and trust management for autonomic message-oriented middleware," in *Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on*, 2009, pp. 810-817: IEEE.

[38] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2009, pp. 171-188: Springer.

[39] A. Simmonds, P. Sandilands, and L. Van Ekert, "An ontology for network security attacks," in *Asian Applied Computing Conference*, 2004, pp. 317-323: Springer.

[40] A. Razzaq, Z. Anwar, H. F. Ahmad, K. Latif, and F. Munir, "Ontology for attack detection: An intelligent approach to web application security," *computers & security,* vol. 45, pp. 124-146, 2014.

[41] Á. García-Crespo, J. M. Gómez-Berbís, R. Colomo-Palacios, and G. Alor-Hernández, "SecurOntology: A semantic web access control framework," *Computer Standards & Interfaces,* vol. 33, no. 1, pp. 42-49, 2011.

[42] S. Alam, M. M. Chowdhury, and J. Noll, "Interoperability of security-enabled internet of things," *Wireless Personal Communications,* vol. 61, no. 3, pp. 567-586, 2011.

[43] B. A. Mozzaquatro, R. Jardim-Goncalves, and C. Agostinho, "Towards a reference ontology for security in the internet of things," in *Measurements & Networking (M&N), 2015 IEEE International Workshop on*, 2015, pp. 1-6: IEEE.

[44] A. Evesti and E. Ovaska, "Ontology-based security adaptation at run-time," in *Self-Adaptive and Self-Organizing Systems (SASO), 2010 4th IEEE International Conference on*, 2010, pp. 204-212: IEEE.

[45] A. Herzog, N. Shahmehri, and C. Duma, "An ontology of information security," *International Journal of Information Security and Privacy (IJISP),* vol. 1, no. 4, pp. 1-23, 2007.

[46] M. Arunadevi and S. Perumal, "Ontology based approach for network security," in *Advanced Communication Control and Computing Technologies (ICACCCT), 2016 International Conference on*, 2016, pp. 573-578: IEEE.

[47] M. Dawson, M. Eltayeb, and M. Omar, *Security Solutions for Hyperconnectivity and the Internet of Things*. IGI Global, 2016.

[48] O. Olawumi, A. Väänänen, K. Haataja, and P. Toivanen, "SECURITY ISSUES IN SMART HOME AND MOBILE HEALTH SYSTEM: THREAT ANALYSIS, POSSIBLE COUNTERMEASURES AND LESSONS LEARNED," *INTERNATIONAL JOURNAL ON INFORMATION TECHNOLOGIES AND SECURITY,* vol. 9, no. 1, pp. 31-52, 2017.

[49] S. Yoon, H. Park, and H. S. Yoo, "Security issues on smarthome in IOT environment," in *Computer Science and its Applications*: Springer, 2015, pp. 691-696.

[50] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, 2014, pp. 1-8: IEEE.

[51] M. Abomhara and G. Kien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security,* vol. 4, pp. 65-88, 2015.

[52] N. F. Noy and D. L. McGuinness, "Ontology development 101: A guide to creating your first ontology," ed: Stanford knowledge systems laboratory technical report KSL-01-05 and Stanford medical informatics technical report SMI-2001-0880, Stanford, CA, 2001.