Security of Ontology In IOT Environments

V.Sudha[1], Ms.S.V.Durggapriya(AP)[2]
[1, 2] Dept of CSE
[1, 2] Sembodai Rukmani Varatharajan Engineering College,
Sembodai,Vedaranyam(tk),Nagapattinam(dt).

Abstract- *The diversity of wireless technologies, connected to the Internet and the more powerful and smaller embedded devices, allows to encompass services to improve everyday activities around us through new applications and businesses. The emerged with the Internet of Things (IoT), where different technologies connected with the Internet provide several applications to change people's lifestyle. However, such integration of heterogeneous devices causes many problems of security and privacy due vulnerabilities of technologies, carrying important consequences to the users of IoT technologies. proposed a reference ontology (IoTSec) with security concepts of M2M communications to help find secure solutions to the IoT environment. Followed a literature review and MENTOR methodology to gather and harmonize security ontologies and knowledge of vulnerabilities, which are the root causes for problems of all information security. In order to elucidate our approach, describe a case study about the applicability of IoTSec in the industrial scenario.*

Keywords- Internet of things; Industrial internet of things, Mentor Methodology.

I. INTRODUCTION

Internet of Things (IoT) is considered the new wave of information industry after of the computer and Internet. This attribution belongs the growth of many different technologies and services and it is employed in several things around of us, combining several standards (M2M –

Machine-to-Machine architecture) such as RFID, Zigbee, Wi-Fi, 3G, embedded devices and sensing devices to ensuring the benefits of smart environmental monitoring, weather forecasting, transportation, healthcare, business, etc.

This heterogeneity of devices and interconnection of smart objects uniquely addressable increase the security threats on the Internet. The main problem of IoT security is the high interaction between humans, machines, and robots and IoT technologies with constraints in terms of connectivity, computational power and energy. In contrast, several security models and trust management, identity management, security mechanisms for protection are defined to ensure the privacy and security goals such as availability, confidentiality, and integrity. In addition to traditional security properties, a security framework is fundamental to make secure the IoT environment allowing do queries and inferences to the security issues.

Information security is an important requirement to fully adoption of IoT applications and must be considered by information system designers and by administrators of organizations that depends on the correct management of information security and confidentiality. However, IoT is still in a conceptual phase, but the field is very dynamic and security challenges are less structured, somewhat organized causing confusion amongst concepts and terms to software developers. Ontology characterizes an interest domain with classes and relationships among them and implements a data model to share a common base knowledge in the particular domain. The application of ontology in information security improves the prediction and assessment of security risk management and computer attacks detection. Reference ontology in the security community has been identified as an important challenge and also for the Internet of Things. In the literature, some works proposed security ontologies general, security ontologies in a specific domain and an ontology-based approach to improve the security to the M2M architecture.

The authors contribute towards a reference ontology for IoT security, unifying concepts and clarifying relationships among different terms. The proposed ontology is not an all-encompassing ontology of the security in IoT, neither was designed to overlap existing ontology and other types of knowledge bases. Our propose is to approximate two specific fields to help the problematic of security in iot and find new secure solution to protect communications among smart devices.

IOT security involves a study to explore the state of the art in vulnerabilities IoT technologies and knowledge acquisition. The methodology MENTOR explore the existing security ontology and a literature reviews to gather and unify similar terms to the glossary and thesaurus. The authors validate the concept in a real world scenario where the reference ontology feeds a security frameworks that interfaces the relationships among collaborating enterprises and devices.

A state of the art on the information security and Internet of Things to evaluate and it to the analyze previous published works in the relevant topic of interest. This strategy allows from approaching the concepts around of different perspectives of this area. The important phase of the literature review is to extract needed information and use as input of methodology MENTOR to create the reference ontology and identify research area gaps, highlighting subjects for future works of investigation and projects.

Methodology for Enterprise Reference Ontology Development (MENTOR) is a methodology to support the development of common reference ontology and assist the semantic transformations among different ontologies. This methodology is composed by two phases: Lexicon Settlement (Phase 1) and Reference Ontology Build (Phase 2).The first phase represents a domain knowledge acquisition, which could be represented in a semantic organized structure with definitions. In this phase creates the thesaurus and glossary using terminology gathering in order to establish the lexicon of a specific domain. The second phase involves the build of the reference ontology and the semantic mappings between existing ontologies. In first moment of this phase, existing ontologies and other types of knowledge representation can be used as input to harmonization ontology process together of thesaurus and glossary. According to, the harmonization method used in MENTOR is proposed from Noy et al. adopted specific phases of the MENTOR methodology to build process and domain knowledge acquisition such as glossary and thesaurus building and ontologies harmonization. These mechanisms are extremely important to identify concepts and their relationships to build reference ontology.

II. RELATED WORK

The IoT system work states the benefit of transitioning from taxonomies to ontologies and proposes an ontology specifying a model of computer attack using DAMLJessKB3 to implement the ontology. This ontology describes the most common attacks are the result of malformed input exploiting a software vulnerability of a network.

The designed STAC ontology with the state of the art of wireless communications (cellular, wireless, wired), devices (sensor or mobile phone) and applications (programming language, framework, database). This work combines existing security ontologies according different domains to provide an approach to help software designers to secure their M2M applications.

A security ontology focused on representing Role-Based Access Control (RBAC) policies to access control based on knowledge-oriented descriptions. The ontology Security Ontology is composed by classes, properties and rules. Classes compose a basic hierarchy of main concepts such as: resources, owners, roles, permissions (read, write and execution) and permission to the current resource, consults. The properties are the relations between the classes such as: has Role, is Onwer Of, its Owner Is, has Permission, has Child, is Child Of, resource, permission.

An ontological approach to enhancing the semantic web with information security. Classes of high level security concepts and relationships between them compose the ontology "OWL-S Security and Privacy". The first sub-ontology defined is Authentication, which has subclasses related and specialized, for example, Public key, X.509 Certificate, and One Time Password. The second sub ontology is considered specify general security notations as Security Mechanisms.

Security Ontology to provide a unified and formal knowledge using an ontological structure for information security domain. The ontology contains 500 concepts and 600 formal restrictions that are represented by either graphical, textual, or description logics representation and the code ontology follow the OWL-DL (W3C Web Ontology Language) standard.

Ontology is a potential tool largely utilized for structuring area of interest. According to study of state of the art, several existing security ontologies have been proposed in the literature and point to different categories such as general security ontology and security ontology applied to specific domain. Some ontologies address only one part of security domain (e.g. computer attacks) and others explore overview of information security. shall present a brief description of the overview of the security ontologies found.

III. FRAMEWORK OVERVIEW

The Sec IoT is an authorization framework that can answer security queries efficiently based on the requesters roles in an Internet of Things context. It consists of 1) Security Mechanism 2) Vulnerability 3)Threats 4) Types of defense 5) Severity Scale.

A. Modeling Process of the Reference Ontology

System design concentrates on moving from problem domain to solution domain. This important phase is composed of several steps. It provides the understanding and procedural

details necessary for implementing the system recommended in the feasibility study. Emphasis is on translating the performance requirements into design specification.

The design of any software involves mapping of the software requirements into Functional modules. Developing a real time application or any system utilities involves two processes. The first process is to design the system to implement it. The second is to construct the executable code.

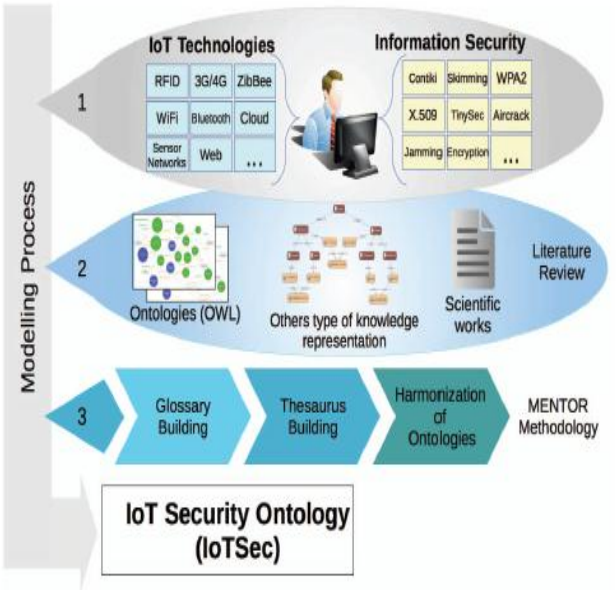

Fig.1-Modeling process of the reference ontology for security in IoT.

Methodology for Enterprise Reference Ontology Development (MENTOR) is a methodology to support the development of common reference ontology and assist the semantic transformations among different ontologies. This methodology is composed by two phases: Lexicon Settlement (Phase 1) and Reference Ontology Build (Phase 2). The first phase represents a domain knowledge acquisition, which could be represented in a semantic organized structure with definitions. In this phase creates the thesaurus and glossary using terminology gathering in order to establish the lexicon of a specific domain.

The second phase involves the build of the reference ontology and the semantic mappings between existing ontologies. In first moment of this phase, existing ontologies and other types of knowledge representation can be used as input to harmonization ontology process together of thesaurus and glossary. According to, the harmonization method used inMENTOR is proposed from No yet al adopted specific phases of the MENTOR methodology to build process and domain knowledge acquisition such as glossary and thesaurus building and ontologies harmonization. These mechanisms are extremely important to identify concepts and their relationships to build reference ontology.

IV. IOT SECURITY ONTOLOGY

Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements. Select methods for presenting information. Create document, report, or other formats that contain information produced by the system.

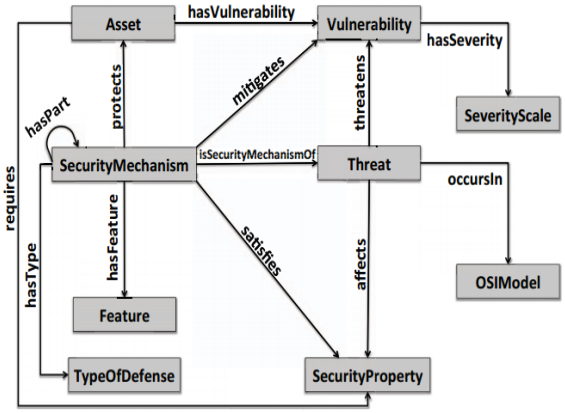

Fig. 2- Ontology For Security In Iot .

V. CONCLUSION

The presented reference ontology for security in IoT based on modeling process to unify concepts and clarify relationships among main basic components of risk analysis of information security. The overview of top-level classes was reorganized to create the enough formalism to represent knowledge base of information security in IoT. This approximation between these areas is the key point to explore the problematic of improve communications of smart objects. IoTSec reference ontology facilities the formalism of the structured knowledge of the security in IoT and it could be used as support of development of new IoT applications and knowledge base to understand the relationships among main concepts of this context. Considering the construction and the validation of the model underlying the measurement process is based on a prior knowledge, it leverages the measurement actions to identify anomalous behaviour and suggest new security approaches (e.g. intrusion detection systems).

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] S. Sicari, a. Rizzardi, L. a. Grieco, and a. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Comput. Networks, vol. 76, pp. 146–164, Nov. 2014.

[3] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Comput. Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[4] Z. Yan and P. Zhang, "A Survey on Trust Management for Internet of Things," J. Netw. Comput. Appl., vol. 42, no. 2, pp. 120–134, 2014.

[5] J. Granjal, E. Monteiro, and J. S. Silva, "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey," Ad Hoc Networks, vol. 24, pp. 264–287, 2014.

[6] G. Dhillon and J. Backhouse. "Technical opinion: Information system security management in the new millennium." Communications of the ACM 43.7 (2000): 125-128.

[7] H. Mouratidis, Integrating Security and Software Engineering: Advances and Future Visions: Advances and Future Visions. IGI Global, 2006.

[8] A. Herzog, N. Shahmehri and C. Duma. "An ontology of information security." International Journal of Information Security and Privacy 1.4 (2007): 1-23.

[9] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," Proc. 4th Int. Symp. Information, Comput. Commun. Secur. - ASIACCS'09, p. 183, 2009.

[10] J. Under coffer, A. Joshi, and J. Pinkston, "Modeling Computer Attacks: An Ontology for Intrusion Detection," pp. 113–135, 2003.