Ontology Based-Security Issues for Internet of Thing (IoT): Ontology Development

Amir Mohamed Talib

Information Technology Department, College of Computer and Information Sciences,
Al Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia

Summary
The use of sensors and actuators as a form of controlling cyber-physical systems in resource networks has been integrated and referred to as the Internet of Things (IoT). However, the connectivity of many stand-alone IoT systems through the Internet introduces numerous security challenges as sensitive information is prone to be exposed to malicious users. In this paper, IoT based-security issues ontology is proposed to collect, examine, analyze, prepare, acquire and preserve evidence of IoT security issues challenges. Ontology development has consists three main steps, 1) domain, purpose and scope setting, 2) important terms acquisition, classes and class hierarchy conceptualization and 3) instances creation. Ontology congruent to this paper is method that will help to better understanding and defining terms of IoT based-security issue ontology. Our proposed IoT based-security issue ontology resulting from the protégé has a total of 44 classes and 43 subclasses.

Key words:
Internet of Thing (IoT), Data Security, Information Security , Cyber Security, Ontology, Protégé and Web Ontology Language

1. Introduction

The term Internet of Things (IoT) grew to become famous in the late 1990s after having a number of technologies related with sensor improvement and machine control, related to the World Wide Web [1]. However, latest trends in wi-fi sensor networks and Industry four inspired the enlargement of IoT purposes to unique domains. Manyika [2] argues that IoT technologies have the capability to attain a total financial fee of $11.1 trillion with the aid of 2025, a fee that is equal to about 11% of the world economy. As an increase in the adoption of Industry four arises, productivity will raise amongst the manufacturing sectors. Several efforts have been made, which searching for an automatic cyber-physical interconnection between virtual and physical worlds, correlating data from the industrial store flooring with run time remarks from the systems.

Grüber [3] defines ontology as “formal, categorical specification of a shared conceptualization”. A formal ontology specifies a device-readable domain model depicting entities and their inter-entity relationships. It frequently consists of a descriptive section and reasoning technology. The descriptive a section of ontology captures the area from the location experts’ issue of view, expressing area archives in a manner that can be processed through computer systems and be understood by way of way of people. Using reasoning technologies allows new data to be derived from the information contained in ontology.

In this research, Web Ontology Language (OWL) is chosen to characterize security difficulty due to the fact of its strength to categorical which means and semantics and complicated relationships. This area offers a very extensive overview of OWL to aid readers in perception the following sections. Readers that are acquainted with OWL principles need to skip this section. Readers that are fascinated in similarly details of OWL ought to refer to [4-8] for extra information. The fundamental ideas in OWL are classes, individuals and properties. The simple construct in OWL are classes. Classes describe ideas in the expertise domain. Properties can in addition outline relationships between classes, constrain instructions or describe a range of attributes of classes. There are two kinds of properties: object residences and data type properties. Object properties relate instances of one class to instances of any other class. Data type properties relate instances of a class to Resource Description Framework (RDF) literals or XML Schema Data types. There are lots of characteristics that make Protégé a significant decision for our proposed ontology. Protégé helps ontology development, the usage of text mining and natural language processing to extract applicable phrases from the scientific literature that can then be organized, Protégé approves vocabulary designers to capture, refine and eventually formalize their intuitions besides being compelled to deal with distracting logical important points early in the design process.

Security troubles are vital for all contexts with private information exchanges and touchy information, however for IoT has necessary characteristics of a massive situation with excessive new release between humans, machines and IoT technologies. It is justified via heterogeneity of one of a kind clever units related with the Internet. In this context, making sure security of purposes and offerings is

Manuscript received August 5, 2023
Manuscript revised August 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.8.20

essential to enhancing believe and use of the Internet. Therefore, these problems have plausible due to the fact there are quite a few conditions of misunderstood principles around data, information, network and cyber security and IoT. For that, ontology is a potential tool mostly utilized for structuring an vicinity of interest.

Many security ontologies have already been developed for distinctive contexts. The most applicable ones determined all through the research phase of this work are listed in the present IoT based-security issues ontologies below. They have been selected as they are of activity to some of the application domains of IoT, are directly based on IoT, or are used as the base for different ontologies of activity for this paper. To the quality of our efforts, this list is a complete precis of all the applicable works associated to the area of this paper.

2. State of the Art

In this section, a state of the art on the IoT based-security issues ontology to consider and analyze previous published works in the relevant topic of interest is described. This approach lets in approaching the concepts round of different views of this area. This study explores to discover and signify the research area and to set up a base information of IoT security ontology. Proposed IoT based-security issues ontology covers three main IoT security issues which are: IoT based-data security ontology, IoT based-information security ontology and IoT based-cyber security ontology. The necessary section of the literature review is to extract needed information and use to create the reference ontology and identify research areas gaps, highlighting subjects for future works of investigation and projects. According to the state of the art, three existing IoT based-security issues ontology have been chosen in the literature (Figure 1).

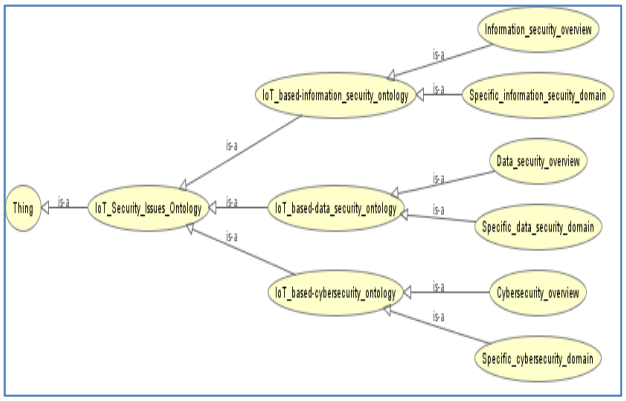

Fig. 1 IoT based-security issues ontology.

3. IoT based-Security Issues Ontology: Existing Ontologies

3.1 IoT based-Data Security Ontology

Denker et al. [9,10] extra than a decade ago, in the frame of Semantic Web Services, described the DAML family of ontologies, covering many security aspects. Authentication, Authorization, AccessControl, DataIntegrity, KeyDistribution and Policy are some of the ideas modelled in super detail. This work, nevertheless, current drawbacks when utilized to the IoT scenario, namely: some of the standards described are out of date or now not relevant to IoT, whilst extra current standards have no longer been brought to the ontology.

Kim et al. [11] mixture a set of associated ontologies below the identify Security Ontology for Annotating Resources, enhancing and making them extensible with the aid of redefining principles for delivered expressiveness. One of the referred ontologies it tries to enhance upon is the DAML ontology which, they state, solely focuses on annotating web services, whereas they center of attention on a extra commonplace “resource annotation”.

Fenz and Ekelhart [12] describe a established Security Ontology, presenting the ontological shape for the area of information security, in addition enriched with concrete expertise of the regarded organization. The ensuing ontology, which carries 500 principles and 600 formal restrictions, equipped in five sub-ontologies, is claimed to help a large vary of data security threat administration approaches. Similar to what will see in following associated works, the vocabulary includes phrases like Assets, Threats, Vulnerabilities, Attacks and Countermeasures, focusing on a widespread security description of the device that should be used as enter in security evaluation processes.

Herzog et al. [13] existing a publicly available, OWL-based ontology of data security which models assets, threats, vulnerabilities, countermeasures and their relations. The ontology can be used as a conventional vocabulary and extensible dictionary of the area of data security.

Gyrard et al. [14] present STACanother security ontology, this time in the context of the ETSI M2M model; constructing a security knowledge base (ontology, dataset and rules) to assist designers impervious M2M purposes all through the sketch phase. Again, it affords a ordinary structures overview of security, this time centered on particular IoT associated technologies, describing Assets, Threats and Security Mechanisms amongst others.

Mozzaquatro et al. [15] presents the IoT Security Ontology (IoTSec), gathering and harmonizing countless associated ontologies (one of which is STAC). This ontology represents understanding about safety in a comparable manner as the preceding work, supplying an extensible and enough data-set (or catalogue of knowledge), and an expressive semantic to signify the security associated traits. It targets at being the reference ontology for security in IoT, incorporating most of the aforementioned ontologies, homogenizing standards throughout them.

De Franco et al. [16] presents SecAOnto: an ontology that formalizes knowledge on safety assessment, focusing on its components and particularities, addressing the relationship between information security and software assessment. Again, it is constructed on pinnacle of STAC and it pursuits at aiding strategies based on rigorous evaluation criteria.

Tao et al. [17] presents an ontology-based security service framework helping security and privacy in interactions, through the use of their ontology of Security that defines a frequent security vocabulary shared by using carrier vendors and customers, and Semantic Web Reasoning Language (SWRL)-based reasoning. This ontology lets in for specific description of the security factors that take phase in communications amongst devices, focusing on the integrity and confidentiality residences of information security by way of describing ideas such as Digital Signature, Encryption, and SecurityToken, associated to information safety and get entry to control.

Choi et al. mannequin a security context ontology [18], on which they base a Power IoT-Cloud security provider framework for its use in strength IoT-Cloud environments. Using quite a number ontological reasoning technologies they are capable to reply to security intrusions intelligently. One greater time, the modelled ontology represents the extraordinary threats, attacks and responses in a way carefully matched to the area problem of power metering, representing some easy ideas like if the consumer has password of if there is some get right of entry to manipulate to a network.

Gonzalez-Gil et al. [19] added an IoT Security Evaluation Ontology (IoTSecEv) primarily based on IoTSec and STAC, aimed at describing security concepts of interest for one of a kind observers, by way of which the security of an IoT system ought to be evaluated, enabling the era of customized rankings with the aid of aid security in IoT aggregators.

Arruda et al. [20] introduces IoT-Privontology, as a light-weight privacy layer that builds upon IoT principles expressed in different ontologies. It makes viable to describe policies and requirements associated to privacy in IoT, permitting for policy evaluation the usage of ontological approaches. Although it doesn't cover elements such as authentication or identification, it does cover some of the get admission to manage matters of activity in this work, particularly these associated with policy-based get entry to control, as nicely as some ideas of information security and accounting.

Priebe et al. [21] leverage semantic reasoning to improve attribute matching on XACML rules by means of imparting an extension of the XACML general in which policies are simplified with the aid of presenting an ontology-based attribute management facility.

Finin et al. [22] find out about the relationship between RBAC and OWL, displaying two different approaches to characterize RBAC mannequin in OWL and later talk about how it can be prolonged to model ABAC.

According to the existing ontologies of IoT based-data security, several existing security ontologies have been proposed in the literature review (Figure 2): data security overview ontologies [9-13, 15, 18, 19] and specific data security domain ontologies [14, 16, 17, 20, 21, 22]

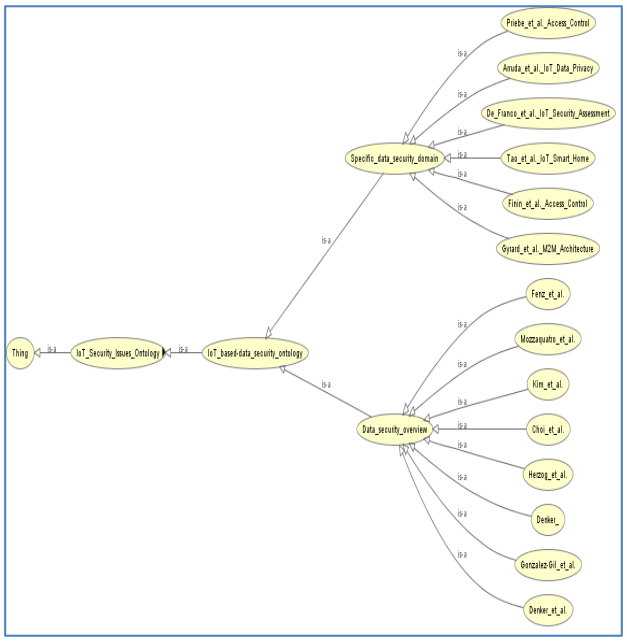

Fig. 2 IoT based-data security ontology.

3.2 IoT based-Information Security Ontology

In this work, Herzog et al. [13] recommend an OWL-based ontology of information security overview to model assets, threats, vulnerabilities, countermeasures and their relations. Ontology is beneficial for reasoning about relationships between entities and it can assist to answer what threats are workable to violate the assets available, for example. Information security ontology involves 88 threat classes, 79 asset classes, 133 countermeasure classes and 34 relations between these classes. The authors describe inference and question language SPARQL (SPARQL Protocol and RDF Query Language) to create views on the ontology. Inference additionally allow explores others countermeasures to manage for a given threat. Furthermore, extensions, technical implementations and tools are working with it. For example, the extension of have an impact on of a threat can be used.

Fenz et al. [12] proposes Security Ontology to grant a unified and formal knowledge the use of an ontological structure for information security domain. The ontology consists of 500 concepts and 600 formal restrictions that are represented with the aid of both graphical, textual, or description logics illustration and the code ontology observe the OWL-DL (W3C Web Ontology Language) standard. Security ontology is composed by way of five sub-ontology, such as: asset, control, vulnerability, threat and security attribute. This structure is primarily based on Landwehr's security and dependability classification [23]. This ontology is utilized in specific strategies to simulation of a variety of attacks [24], security risk analysis [25], information security concept in riskaware commercial enterprise process management [26], holistic IT-security strategy for small and medium sized businesses [27]. Fenz et. al [12] focuses on supplying a model for the whole information security area together with non-core principles such as the infrastructure of an company as well.

Denker et al. [10] advocate an ontological approach to bettering the semantic web with information security. Classes of highlevel security concepts and relationships between them compose the ontology "OWL-S Security and Privacy". The first sub-ontology described is Authentication, which has subclasses associated and specialized, for example, Public key, X.509 Certificate, One Time Password. The second subontology is viewed specify common security notations as Security Mechanisms. Some examples of second sub-ontology are Access Control, Authorization, Data Integrity, Anonymity. The notion of this ontology is offers a foundation for reasoning, read its metadata and using semantic web reasoning methods suggests services to the users. Basically, the authors address the understanding illustration and reasoning issues for believe and security in the semantic web.

Kim et al. [11] proposes the NRL security ontology combination with existing ontologies in different domains and consists of exactly description of protocols, mechanism, goals and others security concepts at more than a few stages of details. This security ontology was once proposed to address the obstacles of present ontologies. In phrases of the business enterprise of subclass relationships, the ontologies are no longer intuitive to apprehend the relations between them and can't categorical all the security information that want be described. Other difficulty highlighted is the lack of expressiveness and the opportunity to describing training different of security associated information. Therefore, the authors enhance these limitations in the NRL security ontology proposed with security information about all sorts of resources, potential to annotate security information in extraordinary environments, effortless to prolong and provide reusability and facility to fit high-level security necessities to lowerlevel capabilities.

Undercoffer et al. [28] states the gain of transitioning from taxonomies to ontologies and proposes an ontology specifying a model of computer attack the usage of DAMLJessKB3 to put into effect the ontology. This ontology describes the most frequent attacks are the end result of malformed enter exploiting a software program vulnerability of a community and the outcome is denial of service. The ontology is composed with classes: host, system component, attack, input, means, enter validation error, common sense take advantage of and consequence.

Gyrard et al. [14] designed the STAC ontology with the state of the art of wireless communications (cellular, wireless, wired), devices (sensor or cell phone) and applications (programming language, framework, database). This work combines current security ontologies in accordance different domains to supply an approach to assist software program designers to tightly closed their M2M applications. This ontology does no longer describe the vulnerabilities of the M2M applied sciences and it solely suggests countermeasures reachable to threats that have an effect on a type of technology.

García-Crespo et al. [29] developed a security ontology targeted on representing Role-Based Access Control (RBAC) policies to get admission to manage primarily based on knowledge-oriented descriptions. The ontology SecurOntology is composed by means of classes, properties and rules. Classes compose a primary hierarchy of fundamental ideas such as: resources, owners, roles, permissions (read, write and execution) and permission to the modern-day resource, consults. The houses are the relations between the classes such as: hasRole, isOnwerOf, itsOwnerIs, hasPermission, hasChild, isChildOf, resource, permission. Finally, the rules are accountable to infer new knowledge, which does no exist in the knowledge base.

Raskjn et al. [30] presents concepts of the Information Security domain, and additionally explains how ontologies can be used to aid the Information Security field, in order to provide a theoretical basis.

Evesti et al. [31] present an ontology to aid the process of measuring Information Security, whereas Feledi & Fenz [32] present a formalization of information security knowledge, by means of potential of an ontology. According to the authors, they need to make express knowledge, so that it can be integrated and used by using each human beings (human-readable format) and machines (machine-readable format).

A top-level ontology of security requirements is introduced in [33] by means of Salini & Kanmani. Based on this ontology, we can design and improve requirements for electronic voting systems (e-voting). The most important goal of this work is to advise security patterns to facilitate the procedure of figuring out security requirements for e-voting systems. The authors existing particular security properties for e-voting systems, namely: anonymity, disclosability, uniqueness, accuracy, transparency, and noncoercibility.

Gyrard et al. [34] introduces the STACK ontology (Security Toolbox: Attacks & Countermeasures) to resource builders in the design of secure applications. STACK defines security concepts such as attacks, countermeasures, security properties and their relationships. Countermeasures can be cryptographic concepts (encryption algorithm, key management, digital signature, and hash function), security tools, or security protocols. Kotenko et al. [35] develop an ontology of security metrics, especially constructed for the SIEM (Security Information and Event Management) domain.

Salini & Kanmani [36] developed an ontology of security requirements for web applications. This work goals at enabling the reuse of information about security requirements in the improvement of special web applications. Kang & Liang [37] introduces a safety ontology, for use in the software improvement process. The proposed ontology can be used for figuring out security requirements, as a realistic and theoretical basis. Koinig et al. [38] implemented a security ontology for cloud computing and a quick literature review. The authors think about the regulatory requirements contained in specific standards.

Blanco et al. [39] summarize a literature evaluate and proposes a method for integrating ontologies, thru qualitative evaluation of greater mature proposals. Souag et al. [40] highlighted an analysis of present security ontologies and their use in defining requirements. The work is section of a challenge that ambitions to enhance the definition of security requirements the use of ontologies. Blanco et al. [39] and Souag et al. [40] emphasize the significance of previous literature reviews and point to the need of updates.

According to the existing ontologies of IoT based-information security, several existing security ontologies have been proposed in the literature review (Figure 3): information security overview ontologies [23, 27, 30-33, 36, 39, 40] and specific information security domain ontologies [24-26, 28, 29, 34, 35, 37].

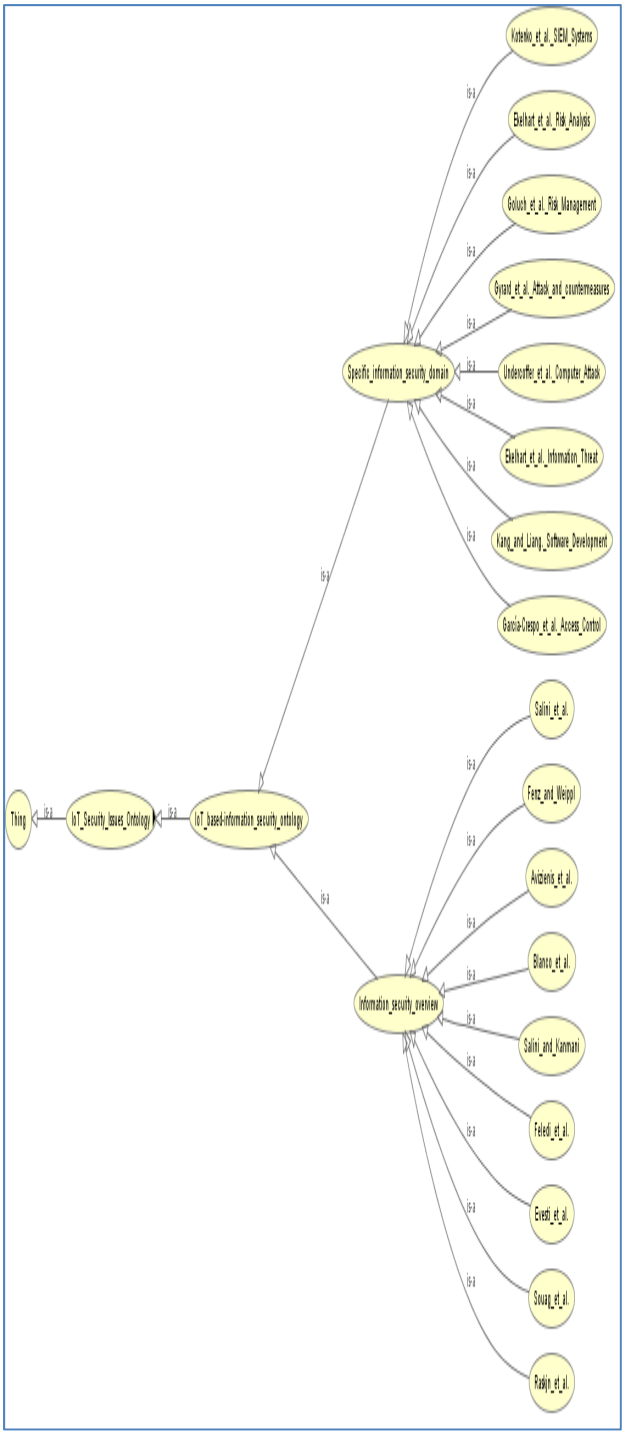

Fig. 3 IoT based-information security ontology.

3.3 IoT based-Cyber Security Ontology

The literature analysis conducted suggests that there are quite a few initiatives to provide cyber security for IoT systems, predominantly through the use of frameworks [17, 41, 42].

Tao et al. [17] proposed an ontology-based security service framework for IoT-based smart homes coping with heterogeneity issues such as security and privacy preservation in a novel multi-layer cloud architectural model and enabling interactions on heterogeneous devices/services. The authors adopted ontologies to model and describe the distinctive components of the IoT assets and a security ontology to acquire the security and privacy upkeep in the system of interactions. However, the authors designed a small ontology thinking about solely security properties (integrity and confidentiality) and the key service (security token) in the method of interactions. They did now not discover the reasoning abilities to infer implicit knowledge on the security ontology, consequently limiting the design of and software of security rules. Our work makes use of a security ontology with a center of attention on the cyber security aspects to provide security services' provisioning based totally on the reasoning capabilities and a model-driven methodology.

Alam et al. [41] proposed a layered structure of IoT to provide secure access provisioning to IoT-enabled matters and interoperability of security attributes between wonderful administrative domains. They used a semantically more desirable overlay to interlink layers, in which the ontology reasoning and semantic guidelines enabled the security aspects in a machine-to-machine platform. However, the authors solely targeted on security requirements of the get entry to manage issues, i.e., the semantic rules have been designed to make sure access authorization. In contrast, our work can perceive and furnish security services the use of the ontology, with reasoning and querying capabilities.

The authors, Ekelhart et al. [42] proposed a framework for information security risk management to measure security via risk assessment, risk mitigation and evaluation. This protected the presentation of a new methodology, AURUM, used to aid the risk management preferred the use of an ontological information security knowledge base to provide a steady and complete technique for the risk manager. This proposal is restrained in the sense that it focuses totally on risk management.

According to the existing ontologies of IoT based-cyber security, several existing security ontologies have been proposed in the literature review (Figure 4): cyber security overview ontologies [41] and specific cyber security domain ontologies [17, 42].

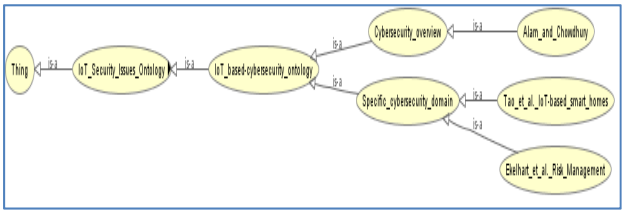

Fig. 4 IoT based-cyber security ontology.

4. IoT based-Security Issues Ontology: Classes and Subclasses

Our proposed IoT based-security issues ontology resulting from the Protégé development process as illustrated below in (Figure. 5). has a total of 44 main classes and 43 sub classes. The ontology is translated in OWL-DL, and cardinality constraints, as well as functional properties are well defined.

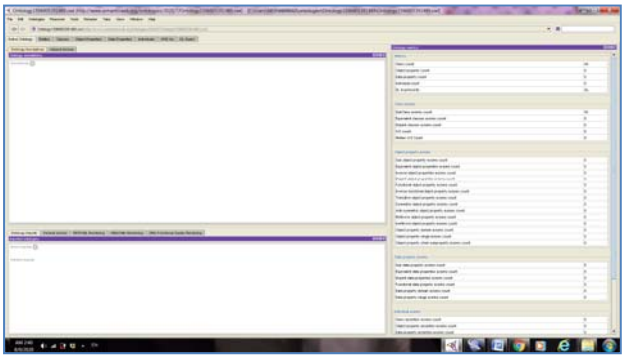

Fig. 5 Number of the 44 main classes and 43 subclasses.

5. Conclusion

An IoT ontology-based security issues to consider and analyze previous published works in the relevant topic of interest is presented. In this context, the proposed ontology is responsible to shows a representation of structured knowledge using semantic web technologies in the context of data security, information security and cyber security. A prototype system was developed using the Protégé. The prototype was based on the principles discussed in this paper and is being tested. The results gained from evaluating this system will help us choose the appropriate ontology according to the main security issue. Finally, hope that this ontology will be a trigger for discussions leading to even more detailed and acceptable ontologies in the domain of IoT based-security issues.

References

[1] J. E. Ibarra-Esquer, F. l. F. Gonzalez-Navarro, B. L. Flores-Rios, L. Burtseva, and M. A. Astorga-Vargas, "Tracking the evolution of the internet of things concept across different application domains," *Sensors,* vol. 17, p. 1379, 2017.

[2] M. James, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, "The internet of things: Mapping the value beyond the hype," *McKinsey Global Institute,* vol. 3, 2015.

[3] T. R. Gruber, "A translation approach to portable ontology specifications," *Knowledge acquisition,* vol. 5, pp. 199-220, 1993.

[4] D. L. McGuinness and F. Van Harmelen, "OWL web ontology language overview," *W3C recommendation,* vol. 10, p. 2004, 2004.

[5] A. M. Talib, R. Atan, R. Abdullah, and M. A. A. Murad, "Security ontology driven multi agent system architecture for cloud data storage security:: Ontology development," *International Journal of Computer Science and Network Security (IJCSNS),* vol. 12, p. 63, 2012.

[6] Z. D. Eri, R. Abdullah, M. A. Jabar, M. A. A. Murad, and A. M. Talib, "Ontology-based virtual communities model for the knowledge management system environment: ontology design," in Ontology-Based Applications for Enterprise Systems and Knowledge Management: IGI Global, 2013, pp. 343-360.

[7] A. M. Talib and F. O. Alomary, "Towards a Comprehensive Ontology Based-Investigation for Digital Forensics Cybercrime," International Journal on Communications Antenna and Propagation, vol. 5, pp. 263-268, 2015.

[8] A. M. Talib, F. O. Alomary, H. F. Alwadi, and R. R. Albusayli, "Ontology-Based Cyber Security Policy Implementation in Saudi Arabia," Journal of Information Security, vol. 9, pp. 315-333, 2018.

[9] G. Denker and L. Kagal, "Security Annotation for DAML web services," in Proc. 2nd International Semantic Web Conference (ISWC2003), Sanibel Island, Florida, USA, 2003.

[10] G. Denker, L. Kagal, and T. Finin, "Security in the Semantic Web using OWL," Information Security Technical Report, vol. 10, pp. 51-58, 2005.

[11] A. Kim, J. Luo, and M. Kang, "Security ontology for annotating resources," in OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", 2005, pp. 1483-1499.

[12] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," in Proceedings of the 4th international Symposium on information, Computer, and Communications Security, 2009, pp. 183-194.

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

[14] A. Gyrard, C. Bonnet, and K. Boudaoud, "An ontology-based approach for helping to secure the ETSI machine-to-machine architecture," in 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), 2014, pp. 109-116.

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

[16] F. de Franco Rosa, M. Jino, and R. Bonacin, "Towards an ontology of security assessment: A core model proposal," in Information Technology-New Generations: Springer, 2018, pp. 75-80.

[17] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," Future Generation Computer Systems, vol. 78, pp. 1040-1051, 2018.

[18] C. Choi and J. Choi, "Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service," IEEE Access, vol. 7, pp. 110510-110517, 2019.

[19] P. Gonzalez-Gil, A. F. Skarmeta, and J. A. Martinez, "Towards an ontology for iot context-based security evaluation," in 2019 Global IoT Summit (GIoTS), 2019, pp. 1-6.

[20] M. F. Arruda and R. F. BulcÃ£o-Neto, "Toward a lightweight ontology for IoT privacy," in Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, 2019, pp. 880-888.

[21] T. Priebe, W. Dobmeier, and N. Kamprath, "Supporting attribute-based access control with ontologies," in First International conference on availability, reliability and security (ARES'06), 2006, pp. 8 pp.-472.

[22] T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W. Winsborough, and B. Thuraisingham, "R OWL BAC: representing role based access control in OWL," in Proceedings of the 13th ACM symposium on Access control models and technologies, 2008, pp. 73-82.

[23] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. "Basic concepts and taxonomy of dependable and secure computing." Dependable and

Secure Computing, IEEE Transactions on 1.1 (2004): 11-33.
[24] A. Ekelhart, S. Fenz, M. D. Klemen and E. R. Weippl. Security ontology: Simulating threats to corporate assets. Springer Berlin Heidelberg, 2006.
[25] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security ontologies: Improving quantitative risk analysis," Proc. Annu. Hawaii Int. Conf. Syst. Sci., 2007.
[26] G. Goluch, A. Ekelhart, S. Fenz, S. Jakoubi, S. Tjoa, and T. Muck, "Integration of an ontological information security concept in risk aware business process management." Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. IEEE, 2008.
[27] S. Fenz, and E. Weippl. Ontology based IT-security planning. IEEE, 2006.
[28] J. Undercoffer, A. Joshi, and J. Pinkston, "Modeling Computer Attacks : An Ontology for Intrusion Detection," pp. 113–135, 2003.
[29] A. García-Crespo, J. M. Go´mez-Berb´ıs, R. Colomo-Palacios, and G. Alor-Herna´ndez, "SecurOntology: A semantic web access control framework." Computer Standards & Interfaces 33.1 (2011): 42-49.
[30] V. Raskin, C. F. Hempelmann, K. E. Triezenberg, and S. Nirenburg, "Ontology in information security: a useful theoretical foundation and methodological tool," in Proceedings of the 2001 workshop on New security paradigms, 2001, pp. 53-59.
[31] A. Evesti, R. Savola, E. Ovaska, and J. KuusijÃ¤rvi, "The design, instantiation, and usage of information security measuring ontology," in MOPAS 2011, The Second International Conference on Models and Ontology-based Design of Protocols, Architectures and Services, 2011, pp. 1-9.
[32] D. Feledi and S. Fenz, "Challenges of web-based information security knowledge sharing," in 2012 Seventh international conference on availability, reliability and security, 2011, pp. 514-521.
[33] P. Salini and S. Kanmani, "A knowledge-oriented approach to security requirements engineering for e-voting system," International Journal of Computer Applications, vol. 49, 2012.
[34] A. Gyrard, C. Bonnet, and K. Boudaoud, "The stac (security toolbox: attacks & countermeasures) ontology," in Proceedings of the 22nd International Conference on World Wide Web, 2013, pp. 165-166.
[35] I. Kotenko, O. Polubelova, I. Saenko, and E. Doynikova, "The ontology of metrics for security evaluation and decision support in SIEM systems," in 2013 International Conference on Availability, Reliability and Security, 2013, pp. 638-645.
[36] P. Salini and S. Kanmani, "Ontology-based representation of reusable security requirements for developing secure web applications," International Journal of Internet Technology and Secured Transactions, vol. 5, pp. 63-83, 2013.
[37] W. Kang and Y. Liang, "A security ontology with MDA for software development," in 2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2013, pp. 67-74.
[38] U. Koinig, S. Tjoa, and J. Ryoo, "Contrology-an ontology-based cloud assurance approach," in 2015 IEEE 24th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2015, pp. 105-107.
[39] C. Blanco, J. Lasheras, E. Fernandez-Medina, R. Valencia-Garcia, and A. Toval, "Basis for an integrated security ontology according to a systematic review of existing proposals," Computer Standards & Interfaces, vol. 33, pp. 372-388, 2011.
[40] A. Souag, C. Salinesi, and I. Comyn-Wattiau, "Ontologies for security requirements: A literature survey and classification," in International conference on advanced information systems engineering, 2012, pp. 61-69.
[41] S. Alam, M. M. R. Chowdhury, and J. Noll, "Interoperability of security-enabled internet of things," *Wireless Personal Communications,* vol. 61, pp. 567-586, 2011.
[42] A. Ekelhart, S. Fenz, and T. Neubauer, "Aurum: A framework for information security risk management," in *2009 42nd Hawaii International Conference on System Sciences*, 2009, pp. 1-10.

Amir Mohamed Talib is an Assistant Professor in Information Technology Department, College of Computer and Information Sciences at Al-Imam Muhammad Ibn Saud Islamic University, Riyadh, Kingdom of Saudi Arabia (KSA). He holds a B.Sc in Computer Engineering from Technological & Science University, Sudan (2006), M.Sc in Computer Science from Universiti Putra Malaysia (2009), and PhD in Software Engineering field at Faculty of Computer Science and Information System at Universiti Putra Malaysia (2012). He has more than 4 years of teaching experience and with about 3 years of system development experience as a system developer at Ejtihad Company, Malaysia. He currently teaches system analysis and design, and software engineering course at both undergraduate and graduate levels. His research interests include Knowledge Management, Information and Network Security, Software Engineering, Computer Supported Collaborative of Work, and Workflow Management. He has also published and wrote books, articles, and technical papers in numerous journals and conference proceedings with regards to his research interest.