Ontology-Based Knowledge Representation in the IoT Cybersecurity System

Anna Bryniarska [a,*] and Waldemar Pokuta [a]

[a] *Faculty of Electrical Engineering, Automatic Control and Informatics, Opole University of Technology, Opole, Poland*
E-mails: a.bryniarska@po.edu.pl, w.pokuta@po.edu.pl

Abstract. The use of Semantic Web in cybersecurity systems is becoming more and more popular. This is an important problem, especially in times when IoT systems are developing very quickly and and their security must be maintained. Thanks to the semantic web, it is possible to store and process cybersecurity knowledge using ontology. We describe a system for analyzing the level of cybersecurity among Polish citizens, in particular Internet of Things (IoT) users. An ontology-based knowledge representation related to the security level was created for the described system. The ontology contains the information necessary to determine the security level in different locations and to conduct deeper analysis. It has been prepared for the needs of the IoT system for storing data and knowledge. The described Semantic Web application is part of a larger project that allows to determine cyber security and cyber threats of IoT devices.

Keywords: semantic web, internet of things, cyber security, ontology, ontology-based system

1. Introduction

Along with the development of the Internet of Things (IoT), the field of cybersecurity of devices located in the IoT is also developing very rapidly. Devices connected to a common network can see each other and unauthorized persons can access these devices [1]. This may lead to a security breach or leakage of sensitive data. IoT can bring many benefits, such as accessibility, integrity, availability, scalability, confidentiality, and interoperability. Nowadays, more and more such systems are used in various applications. However, we must be aware of the safety of IoT devices.

Semantic Web (SW) is more and more often used in various fields of science, including systems related to cybersecurity systems [2–8]. Moreover, SW are also widely used in IoT systems. In the literature, you can find applications, for example, in health care, agriculture or smart homes [9–13]. Due to the fact that the subject of cybersecurity is a very important issue, in particular when considering IoT systems, we present the possibility of using SW in this subject. This is a new approach where SW has been designed and created to support the process of determining the level of cybersecurity. The main goal is to determine the level of cybersecurity in a given location based on aggregated data collected during network scanning. During scanning, we receive information about IoT devices connected to the network and some information about their properties, technologies or features used. This is possible thanks to the collection of data from many devices and scans carried out by users. The assumption is that the user will carry out network scans in order to ensure his safety in this network. This data will be further transmitted and analyzed

[*] Corresponding author. E-mail: a.bryniarska@po.edu.pl.

using the SW. The involvement of many millions of users is part of Mobile Crowdsourcing (MCS). One of the application of MCS is crowdsensing. Crowdsensing, consisting in collecting data from many mobile devices of users and analyzing the surrounding real world based on this data [14, 15]. Moreover, human-machine interaction becomes a large challenge in crowded environments [16]. The use of systems that allow intelligent processing of data in such a crowded environment is an important aspect.

SW provides the possibility of creating complex schemas, which can be used to design relationships between objects in the real world. These relationships can be of different types: hierarchical, causal, functional, temporal, and others. However, the flexibility of this tool can lead to difficulties in searching for knowledge organized in this way [17]. To address the problems related to efficiency, clustering mechanisms (such as K-NN or K-means) are sometimes used. A related method for reducing the complexity of the problem of searching for data in semantic web is data granulation, where a representative is designated for each data group, called a granule [18–20].

In the paper we present an overview of the use of ontology-based architecture for IoT systems. Then we describe cybersecurity systems that use ontologies to store and process knowledge. We also describe the cybersecurity system which, among other things, allows you to determine the level of security of scanned devices. Part of this system is the semantic web which was created for the needs of this system. The created ontology is presented in detail and metrics of this SW were created. Next, the future application possibilities and the use of this ontology for particular tasks are described.

2. Semantic Web for IoT

In the IoT systems, data are collected from sensors of some devices connected to the network. IoT systems allow us to develop new services and applications to connect smart objects, integrate network technologies, devices, sensors, software and distinct infrastructures. The so-called Semantic Web of Things (SWoT) is created, where data obtained directly from sensors are stored in the SW and later they are processed by systems [21–23].

Due to the relationship between SW and IoT technologies, a comprehensive review of this topic is needed in the literature. The review paper tries to fill this gap[24]. As an example of the versatile use of SW and IoT, there may be their implementations in intelligent dialogue systems [25] or health care [13, 26].

SW and IoT are commonly used in cloud solutions - an overview of this topic can be found in the review articles [27] (review of Cloud-Driven Semantic Web solutions), [9] and [12] (Semantics for IoT security subchapter). Another review of solutions [2] describes models for detecting, selecting and connecting devices in the IoT network. In addition to review articles, several papers describing specific solutions for the use of SW and IoT in clouds can be distinguished in this group. An example may be the application in agriculture (nut cultivation in Turkey) [28] – the wireless sensor network (WSN) collects information from sensors saved in the form of SW. This information is then processed using SPARQL (a query language and protocol for RDF files). The use of SW to describe IoT devices has been described in [9]. There is a description of SW for the purpose of storing data on Web of Things (WoT) and Semantic Web of Things (SWoT) devices, and the topic of using SW in cybersecurity. A common problem in real-world systems where data is obtained from devices on the network is missing or lost data. The problem of recovering lost data is dealt with in [29]. Another article [21] analyzing the current approach to device description (SWoT) points to the ineffectiveness of the approach in which device descriptions are decentralized and introduces a proposal for a new approach, the information-centric networking.

Another topic present in the literature on the subject is the use of SW and IoT for security. In [30], an ontology for managing the climate crisis and climate change was created. It is a proposal to use a data structure to store and organize the flood of data coming from people and sensors during crisis management. OntoMetrics was used to evaluate the SW, while queries to the network were made using SPARQL. Another paper [31] describes the IoT infrastructure for security in public places, the DESMOS system. GraphDB stores an ontology that contains data such as GPS position and locator signal strength. Applications include: lost child, fainting due to illness, natural disasters. For devices such as automatic vehicles, ontologies are created in which information about the vehicle's surroundings can be stored [32] or information can be exchanged in networks to which vehicles are connected [33]. The issue of secure exchange of information between devices was addressed by the authors of the publication [3]. This article presents a number of ontologies in different domains (Web, MANET, 2G/GSM, 3G/UMTS, 4G/LTE, Wi-Fi, Intrusion Detection System). In this paper, attention was drawn to the fact that ontologies for security are rarely published and are not standardized. Another publication [34] describes an ontology-based reasoning system for devices in an electrical network. The developed system concerns the security of such an IoT system. The proposal of a secure IoT architecture, where data from sensors are saved in the semantic web, was presented in the article [35]. The issue of information exchange of devices in smart homes is described in [36]. Devices from different manufacturers and operating in different standards require a unified standard. An ontology has been developed that stores data in a multi-layered manner. The issue of privacy and security in such networks was also developed. Another publication [37] describes the AURUM tool for company risk management. An OWL-based knowledge base was used to store the data. The next publication describes the use of the semantic web in security systems [38]. This paper presents the problem of automatic (using ontologies) analysis of threats to which the company may be exposed. As can be seen in the literature, there are many applications of semantic webs to IoT data. This proves that the semantic web has great potential in the case of data collected from IoT sensors.

3. Semantic Web in Cybersecurity

The Semantic Web can also be used to record, process and store data related to cybersecurity for the internet of things [39, 40]. Then SW stores data from the security field. IoT systems, due to heterogeneous connectivity, pose many challenges and possible threats. Application of SW to cybersecurity systems for IoT can bring many benefits. SW are based on an ontology in which certain classes are written, but also the relationships that arise between these classes. This enables reasoning based on the ontology.

There are some solutions related to cybersecurity problem in IoT systems based on the ontology [4]. The paper [7] presents a practical example in which a reference ontology was created using the semantic web to describe information on operations carried out in the field of cybersecurity. This solution uses the CVE database offered by the MITER consortium. First, the ontology describes the users of the system and their roles in this system related to protection against cyber threats. The created ontology was described using Description Logic DL. For the prepared ontology, an application with an interface enabling the extraction of information from this web was also created. The solution was developed in cooperation with SOC (Security Operations Center) units working in the USA, Japan and South Korea. A similar system is the CoCoa system described in [5], which refers to the NIST cybersecurity framework and the Cyber Security Operations Center (CSOC). In this ontology, the entire cybersecurity management process is modeled along with the people responsible for these processes. The ontology is used to analyze whether a cybersecurity incident has occurred, i.e. whether an attack has occurred. In [41, 42] also the detection of cybersecurity incidents (IDS system) in cloud computing is considered. It is interesting to use correlations between certain conditions and symptoms to determine whether a device is under attack.

Another complete system related to IoT cybersecurity is the system described in [39]. An ontology-based cybersecurity framework has been proposed that can be used in a company to describe procedures related to maintaining security. The main purpose of creating this framework is to detect intruders (IDS - Intrusion Detection System) trying to get into the resources of a given company. The paper presents the created ontology, the methodology of checking the ontology, and examples of reasoning based on this ontology. In [6] the creation of a single unified ontology language for cybersecurity is presented, the so-called UCO unified cybersecurity ontology. They use RDF files and DL. The most important classes that are described in this ontology are: Means (attack type), Consequences (attack consequences), Attack (attack, attack threat), Attacker (attacker), AttackPattern (description of typical attacks), Exploit (known exploits), Exploit Target (exploit target). The CVE database was used to describe the vulnerability to cyber threats. Examples of queries using the SPARQL language are given.

The paper [43] presents the Cybersecurity Vulnerability Ontology (CVO) and on this basis the Cyber Intelligence Alert (CIA) system was created. This system alerts you when there is a cyberattack. The solution uses the CVE database to describe the vulnerability to threats. The inference rules are presented using the SWRL language. An extensive evaluation and verification of the presented solution was carried out.

An interesting idea was also presented in the paper [44], where a dynamic analysis of the IT system is carried out on the basis of the created ontology. The network administrator checks in real time using this ontology whether a

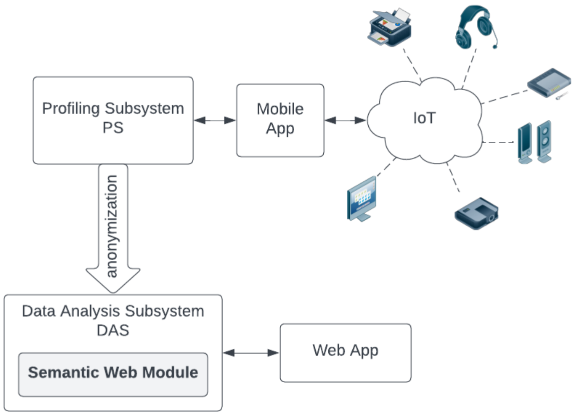

Fig. 1. A schema of the IoT cybersecurity system.

given network is secure at a given moment based on the CVE database. The system informs you if there is a device at a given IP address that can be considered dangerous.

On the other hand, in the paper [38], automatic modeling of threats based on ontology was dealt with. For example, in a given company we check what cyber threats it may be exposed to, but instead of manually determining these threats, it is done automatically based on the data stored in the ontology.

The use of SW in cybersecurity systems, especially for IoT systems, is absolutely justified. The advantages of SW is the recording of knowledge using ontology. Then the knowledge is arranged into classes and individuals that relate to each other.

4. The Cybersecurity System

The cybersecurity system for which the ontology saved with SW will be created is a large system for analyzing data on the security of Polish citizens. The system consists of a mobile application that can be installed on a mobile phone and an analysis module where anonymized data are transferred. These data are subject to further analysis and recording in SW. The system that is being created is much larger and contains many different elements, but in the paper we will focus and describe only the elements related to building ontology and its further use.

The schema of proposed IoT cybersecurity system is presented in Figure 1. A mobile application has been designed in the system that scans the environment. In the network where the phone with the application running is located, all IoT devices connected to it are scanned. The mobile application will have many users who, using it, will be able to scan the network in which their mobile device is located. Then the user will receive a scan report with relevant recommendations. This is the mobile crowdsourcing application running on the MCS system.

The next step is sending data to the profiling subsystem (PS). PS uses cybersecurity expertise to determine certain measures of device security in various aspects. A database is created in which there are individual scans and devices found during these scans. Additionally, each device has a specific metric with safety factors. Cybersecurity experts set these metrics based on their knowledge. Another important data obtained in the MCS system by the mobile application is the location of the scan. This enables data to be grouped according to localization. It is also the module that defines the recommendations for the user.

Then data are anonymized and sent to the data analysis subsystem (DAS). During anonymization, the location of the scanned device is also generalized. In DAS there is a Semantic Web Module (SWM) which contains an ontology-based knowledge representation. The SWM module is described in detail in the following sections of this paper.

The end result of the system operation is the display of the results of the analysis of anonymized and grouped data in the Web Application. The described MCS system allows you to obtain a lot of data that can be grouped. We can do big data research obtained from scans. In the DAS there are also other data analysis modules that are not the subject of these studies and operate independently of SWM.

In Figure 2 a schema of the Semantic Web Module (SWM) is presented. First, the data is sent to the module in the form of a json file. Based on the json file, a semantic web describing this knowledge is created. The structure of the data and SW has been prepared and developed in advance because we know the structure of the input data. the SW schema with examples is described in the ontology section 5. Data and appropriate relations between individuals (instances of given classes) in the SW are only added to the appropriate classes in the SW. In this way, we obtain an ontology describing IoT devices and indicators regarding their security level.

SW prepared in this way is passed on to information granulation. Based on selected cluster analysis algorithms such as k-means, density-based spatial clustering, affinity propagation, knowledge granules will be created. A granule representative will be designated for each granule. In the absence of data for devices within a given information granule, they can be supplemented on the basis of metrics calculated for a representative of this granule. It is essential in the further process of analyzing the security level in the selected location. Then, for a given location, the level of security of IoT devices is calculated, taking into account the synergy between devices. When similar devices with similar safety ratings are present in a given location, the overall level of safety may change. IoT device data can affect each other and overall security level.

During the entire process of SWM operation, all data is saved and retrieved from the ontology in the semantic web. All calculated parameters are further transferred from the semantic web to the database and then to the results presentation module in the web application.

5. Proposed Ontology

The project will apply in practice the theoretical study presented in the papers [45–47]. These papers present a theoretical apparatus for SW, searching for knowledge in this web, also when this knowledge is uncertain or inaccurate.

In the literature, it can be noticed that for practical solutions, the SW is described using the OWL2 or RDF language, based on the structure of xml files. In order to write data to the Semantic Web from the database, the relational database can be mapped to OWL files [48] and otherwise. Often, data from a non-relational database such as Firebase or GraphDB are mapped to JSON format and then to rdf files. The same is the case here. To perform operations on ontology or reasoning in the SW, python or java programming languages are most often used. In this case, data is downloaded from the json file and saved to the ontology-based file based on the schema of this SW prepared earlier.

Very often, for the visualization of owl or rdf files, the Protege program is used, which allows you to display the created ontology using trees or graphs [49]. The Protege program was used to design and create a semantic web schema for the SWM module.

The SW schema includes following classes:

- **ScannedDevice** - represents one scanned IoT device. This is the central class of the Semantic Web schema that is related to the other classes. The class also contains the selected properties obtained from the device during the scan.
- **Scan** - a class that contains information about the scan execution time and location.
- **MapLocation** - the class contains information about the location of the scanned device. Due to the anonymization of data, the location has been quantized. Locations on the map have been saved using areas to which devices are assigned.
- **DeviceType** - a class that contains information about the type of device, e.g. printer, camera, smartwatch, headphones, etc.
- **DeviceManufacturer** - class containing information about the manufacturer of the device.
- **DeviceModel** - the class contains the name of the device model that was given to the device by the manufacturer.
- **DeviceFirmware** - class containing the name of the firmware version contained in the device.

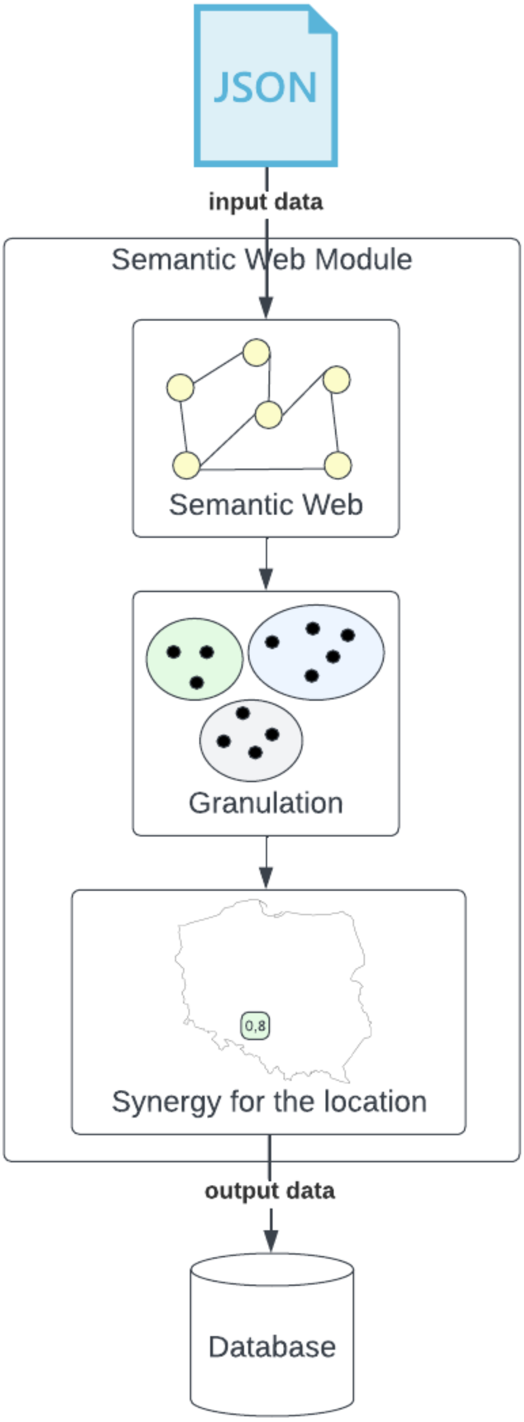

Fig. 2. A schema of the Semantic Web Module.

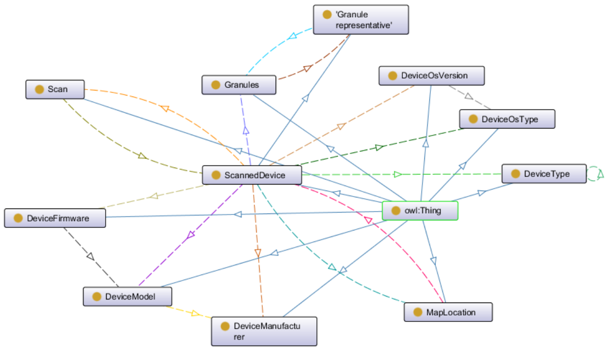

Fig. 3. A schema of the Semantic Web.

- **DeviceOsType** - the class contains the name of the operating system type that has been installed on the device.
- **DeviceOsVersion** - the class contains the version name of the operating system installed on the device.
- **Granule** - a class that groups scanned devices into granules. Granules are used in the next stages of SWM and will be part of further research.
- **GranuleRepresentative** - a representative of a granule that has the most characteristic properties for devices belonging to the granule.

In addition to the associations of the listed classes with the class that represents scanned devices *ScannedDevice*, there are some associations between the classes related to the hierarchy of features of these devices. As part of these associations in the Semantic Web, there are associations between the *DeviceManufacturer, DeviceModel* and *DeviceFirmware* classes and between the *DeviceOsType* and *DeviceOsVersion* classes. The *DeviceType* class is related to itself due to the fact that there may be subtypes of devices, e.g. printer - laser printer or vacuum cleaner - washing vacuum cleaner.

In OWL or RDF support a set of axioms for stating assertions. Assertions are axioms about individuals that are often also called facts. Assertions are implemented by object properties. In presented SW the object properties are:

- **isIn** – connects the *ScannedDevice* class with the *MapLocation* class and is inverse to property *contains*. It is a functional property, it means that scanned device is only in one location on the map.
- **contains** – relationship between *MapLocation* and *ScannedDevice* and is inverse to property *isIn*.
- **hasScannedDevice** – connects the *Scan* class with the *ScannedDevice* class and is inverse to property *isFoundDuring*. It is a functional property, it means that during the scan each device can be found only once.
- **isFoundDuring** – relationship between *ScannedDevice* and *Scan* and is inverse to property *hasScannedDevice*.
- **isTypeOf** – connects the *ScannedDevice* class with the *DeviceType* class. It is a functional property, it means that the scanned device can have only one type.
- **isSubtypeOf** – connects the *DeviceType* class with itself. Allows us to create a device subtype.
- **hasManufacturer** – connects the *ScannedDevice* class with the *DeviceManufacturer* class.
- **hasModel** – connects the *ScannedDevice* class with the *DeviceModel* class. It is a functional property. It means that the scanned device can have only one model.
- **hasFirmware** – connects the *ScannedDevice* class with the *DeviceFirmware* class.
- **isModelOf** – relationship between *DeviceModel* and *DeviceManufacturer* and indicates a link between manufacturer and model of device.
- **isFirmwareOf** – relationship between *DeviceFirmware* and *DeviceModel* and indicates a link between firmware and model of device.
- **hasOsType** – connects the *ScannedDevice* class with the *DeviceOsType* class.
- **hasOsVersion** – connects the *ScannedDevice* class with the *DeviceOsVersion* class.
- **isVersionOf** – relationship between *DeviceOsVersion* and *DeviceOsType* and indicates a link between OS version and type of device.

General	
Axioms	418
Logical axioms count	309
Class count	11
Object property count	18
Data property count	70
Properties count	88
DL expressivity	ALHIF(D)
Class axioms	
SubClassOf axioms count	1
Object property axioms	
SubObjectPropertyOf axioms count	15
Inverse object properties axioms count	3
Functional object properties axioms count	8
Inverse functional object properties axioms count	1
Object property domain axioms count	17
Object property range axioms count	17
Data property axioms	
SubDataPropertyOf axioms count	64
Functional data property axioms count	64
Data property domain axioms count	62
Data Property range axioms count	57
Annotation axioms	
Annotation assertion axioms count	11

Table 1

Metrics genereted for SW by the OntoMetrics tool

- **belongsToGranule** – connects the *ScannedDevice* class with the *Granules* class. It is a functional property. It means that the scanned device may belong to only one granule.
- **hasRepresentative** – connects the *Granules* class with the *GranuleRepresentative* class and is inverse to property *isGranuleRepresentativeOf*. It is a functional property. It means that granule has only one representative.
- **isGranuleRepresentativeOf** – connects the *GranuleRepresentative* class with the *Granules* class and is inverse to property *hasRepresentative*. It is a functional and inverse functional property.

Data properties are also defined in SW. The instances of the *ScannedDevice* class has functinal data properties *hasName* and *hasOsUpdate*. Additionally, this class instances have 57 data properties that correspond to the relevant metrics containing data on the safety of using this device. These metrics are expressed as values in range between 0 and 1. The proposed metrics are related to such areas as: security assessment of individual layers of the OSI model; assessment of individual device components; the risk of data loss or interception or financial losses; security in accordance with the General Data Protection Regulation in the European Union, vulnerability to threats according to the CVE database etc. These features were developed in PS systems by experts participating in the creation of the whole system. The same metrics were used for the instances of the *GranuleRepresentative* class.

As part of data properties, we have created two properties *hasLocationTotalSecurityScore* and *hasLocationTotalSynergySecurityScore* for the instances of the *MapLocation* class. They will store the calculated safety scores for a given location on the map. The introduced structure of the SW is the basis for conducting further research aimed at visualizing the level of cybersecurity.

To evaluate the finished semantic web, you can use the free OntoMetrics tool from the University of Rostock [50]. The base metrics of SW are presented in Table 1. Base metrics contains simple metrics that show the quantity of ontology elements.

Attribute richness	6.363636
Inheritance richness	0.090909
Relationship richness	0.947368
Attribute class ratio	0.0
Equivalence ratio	0.0
Axiom/class ratio	38.0
Inverse relations ratio	0.04878
Class/relation ratio	0.578947

Table 2

Schema metrics for SW by the OntoMetrics tool

Absolute root cardinality	10
Absolute leaf cardinality	10
Absolute sibling cardinality	11
Absolute depth	12
Average depth	1.090909
Maximal depth	2
Absolute breadth	11
Average breadth	5.5
Maximal breadth	10
Ratio of leaf fan-outness	0.909091
Ratio of sibling fan-outness	1.0
Tangledness	0.0
Total number of paths	11
Average number of paths	5.5

Table 3

Graph metrics for SW by the OntoMetrics tool

Schema metrics are provided in Table 2. They address the design of the ontology. Metrics in this category indicate the richness, width, depth, and inheritance of an ontology schema design. Moreover, graph metrics are presented in Table 3. Graph, also called structural, metrics calculate the structure of ontology.

The individuals assigned to the classes are not described in this paper because the SWM module is launched at certain time intervals. Then, the individuals are each time added to the SW schema for a given time range and the entire module calculates the appropriate security levels for new data. Thus individuals are not part of the SW schema. The processing of individuals will be the subject of further research.

6. Application of the semantic web in the system

This chapter presents plans to use the designed SW in the visualization of the level of cybersecurity of IoT devices in order to increase the efficiency and efficacy of activities in this area.

The actual data from the scanned devices lacks the values of many metrics needed for security analysis. For this reason, the first planned action on this raw data will be to supplement the missing data on the basis of devices of a similar nature. For this purpose, the *Granules* and *GranuleRepresentative* classes have been separated in the SW schema. The granule class will group devices according to known features (this can be done using one of many data clustering methods - e.g. KMeans, Affinity Propagation, MeanShift, Spectral Clustering, Ward, Agglomerative Clustering, DBSCAN, OPTICS, BIRCH, Gaussian Mixture, and others.) so that then, in instances of the granule representative class (related to instances of the granule class), characteristic feature values for devices grouped in a granule will be created.

After filling in the missing metric values of IoT devices, you can determine aggregate information about cybersecurity in a given location and time. Due to the privacy policy, data that comes from mobile devices of individual users are subject to the process of anonymization (personal data) and quantization (location data) before they reach the DAS subsystem and the semantic web module. Therefore, the semantic web module does not have information about the exact location of devices, however, it can tell which devices are in the immediate vicinity based on whether they were scanned during one scan. Such information is valuable due to the likelihood of synergy of threats. Threat synergy occurs when two devices that are moderately vulnerable to hacking can be simultaneously used by a cybercriminal to perform a successful attack. An example of such synergy can be a device on which a password must be entered and another device with a camera in the immediate vicinity - the threat is then greater than the sum of threats for the same devices when they are not adjacent to each other. The synergy of threats can be estimated based on the knowledge of the types and models of devices as well as on the basis of the software (firmware, operating system) on it. Generally, the more data we know about devices, the more accurately we can estimate synergies between them. Data processed in this way will be grouped by location and will be available to persons responsible for counteracting cybercrime.

Another way of using data prepared in this way in the structure of the semantic web is the assessment of cybersecurity for specific devices. Some devices have published information about their vulnerability. However, new models of IoT devices with unknown vulnerabilities are created every day, and although information about them is supplemented cyclically, many months can pass from the moment the device is released on the market until the vulnerability is published. To estimate the probability of vulnerability of an unknown device, data classification algorithms can be used, where the learning data will be the metrics of devices for which the security level has been previously determined. The classification algorithm can be based on one of many tutored learning methods, e.g. Decision Trees, k-Nearest Neighbors, Naive Bayes, Support Vector Machines, Logistic Regression, Neural Networks, Random Forest, etc. The properly classified data can then be presented using a table or tree in which the types and models of devices will be distinguished and the estimated level of vulnerability to cyberattacks for them.

7. Conclusion

In times of the growth of IoT networks, the issue of cybersecurity takes on a different dimension and becomes a key issue. In the paper we described the cybersecurity system collecting data from IoT devices. In order to obtain data, network scans are carried out by many users on many mobile devices. For this mobile crowdsourcing system the semantic web was created. Knowledge from this system was represented by ontology-based representation. The proposed ontology is part of a research project currently in progress. The presented ontology contains data necessary to determine the level of security of Polish citizens collected during network scans in the mobile application of the system. Later, the system can be extended worldwide.

The proposed ontology will be used further in the analysis system to determine the granules of knowledge. Then, on this basis, it will be possible to supplement the missing knowledge. A map of the security level will be prepared for the cybersecurity system, which will use the created ontology and will take into account the synergies between threats in different regions. Building an ontology is the first step to creating a system that will be able to assess the level of security, analyze the synergy taking place in different geographic regions and help supplement the knowledge in case of lack of it.

The presented solution is an innovative method of using semantic web and ontology-based knowledge representation for the MCS system collecting IoT data. The use of ontology introduces new possibilities in data processing. The advantages we get is using the ontology is the expressiveness of OWL which allows to specify logical classes. Ontology introduces a richer representation of knowledge and allow us to use the relationship between classes in calculations.

Acknowledgments

The project is co-financed by the National Center for Research and Development Poland under the CyberSecIdent program "Cybersecurity and e-Identity". Agreement: CYBERSECIDENT/489912/IV/NCBR/2021

References

[1] Y. Lu and L. Da Xu, Internet of Things (IoT) cybersecurity research: A review of current research topics, *IEEE Internet of Things Journal* **6**(2) (2018), 2103–2115.

[2] M.E. Adam, Usages of semantic web services technologies in IoT ecosystems and its impact in services delivery: A survey, *International Journal of Computer (IJC)* **36**(1) (2020), 53–72.

[3] 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)*, IEEE, 2014, pp. 109–116.

[4] Y. Merah and T. Kenaza, Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence, in: *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–8.

[5] C. Onwubiko, Cocoa: An ontology for cybersecurity operations centre analysis process, in: *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, IEEE, 2018, pp. 1–8.

[6] Z. Syed, A. Padia, T. Finin, L. Mathews and A. Joshi, UCO: A unified cybersecurity ontology, *UMBC Student Collection* (2016).

[7] T. Takahashi and Y. Kadobayashi, Reference ontology for cybersecurity operational information, *The Computer Journal* **58**(10) (2015), 2297–2312.

[8] S. Kirrane, S. Villata and M. d'Aquin, Privacy, security and policies: A review of problems and solutions with semantic web technologies, *Semantic Web* **9**(2) (2018), 153–161.

[9] A. Chatzimichail, E. Stathopoulos, D. Ntioudis, A. Tsanousa, M. Rousi, A. Mavropoulos, G. Meditskos, S. Vrochidis and I. Kompatsiaris, Semantic web and iot, *Semantic IoT: Theory and Applications: Interoperability, Provenance and Beyond* (2021), 3–33.

[10] B.A. Dawood and M. Sah, Semantic web and healthcare system in IoT enabled smart cities, in: *Innovations in Smart Cities Applications Volume 4: The Proceedings of the 5th International Conference on Smart City Applications*, Springer, 2021, pp. 546–557.

[11] F. Loukil, C. Ghedira-Guegan, K. Boukadi and A.N. Benharkat, LIoPY: A legal compliant ontology to preserve privacy for the Internet of Things, in: *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2, IEEE, 2018, pp. 701–706.

[12] A. Rhayem, M.B.A. Mhiri and F. Gargouri, Semantic web technologies for the internet of things: Systematic literature review, *Internet of Things* **11** (2020), 100206.

[13] V. Costa Lima, D. Alves, F. Andrade Bernardi and R.P. Charters Lopes Rijo, Security approaches for electronic health data handling through the Semantic Web: A scoping review, *Semantic Web* (2021), 1–14.

[14] Y. Wang, X. Jia, Q. Jin and J. Ma, Mobile crowdsourcing: framework, challenges, and solutions, *Concurrency and Computation: Practice and experience* **29**(3) (2017), e3789.

[15] A. Ray, C. Chowdhury, S. Bhattacharya and S. Roy, A survey of mobile crowdsensing and crowdsourcing strategies for smart mobile device users, *CCF Transactions on Pervasive Computing and Interaction* **5**(1) (2023), 98–123.

[16] B. Klin, M. Podpora, R. Beniak, A. Gardecki and J. Rut, Smart Beamforming in Verbal Human-machine Interaction for Humanoid Robots, *IEEE Robotics and Automation Letters* (2023).

[17] S. Murtaza and S. Ahmed, Impact of the Semantic Web mining by using different techniques-A Survey, *International Journal of Science and Innovative Research* **1**(02) (2020).

[18] A. Bryniarska, A data granulation model for searching knowledge about diagnosed objects, in: *Trends in Advanced Intelligent Control, Optimization and Automation: Proceedings of KKA 2017—The 19th Polish Control Conference, Kraków, Poland, June 18–21, 2017*, Springer, 2017, pp. 681–690.

[19] A. Bryniarska, Information granule system induced by a perceptual system, in: *2019 Federated Conference on Computer Science and Information Systems (FedCSIS)*, IEEE, 2019, pp. 19–27.

[20] A. Bryniarska, Granulation of Technological Diagnosis in the Algebra of the n-Pythagorean Fuzzy Sets, in: *Advanced Information Networking and Applications: Proceedings of the 35th International Conference on Advanced Information Networking and Applications (AINA-2021), Volume 2*, Springer, 2021, pp. 358–369.

[21] M. Ruta and F. Scioscia, Information-centric Semantic Web of Things, *Open Journal of Internet Of Things (OJIOT)* **6**(1) (2020), 35–52.

[22] A. Salama, M.E. Shaheen and H. Alfeel, Rule-based Recommendation System based on Semantic Web of Things, *International Journal of Engineering Research and Technology* **13**(6) (2020), 1455–1465.

[23] S. Botonakis, A. Tzavaras and E.G. Petrakis, iSWoT: service oriented architecture in the cloud for the semantic web of things, in: *Advanced Information Networking and Applications: Proceedings of the 34th International Conference on Advanced Information Networking and Applications (AINA-2020)*, Springer, 2020, pp. 1201–1214.

[24] D. Andročec, M. Novak and D. Oreški, Using semantic web for internet of things interoperability: A systematic review, *International Journal on Semantic Web and Information Systems (IJSWIS)* **14**(4) (2018), 147–171.

[25] Y. Sermet and I. Demir, A Semantic Web Framework for Automated Smart Assistants: A Case Study for Public Health, *Big Data and Cognitive Computing* **5**(4) (2021), 57.

[26] N. Malik and S.K. Malik, Using IoT and semantic web technologies for healthcare and medical sector, *Ontology-Based Information Retrieval for Healthcare Systems* (2020), 91–115.

[27] K.I. Taher, R.H. Saeed, R.K. Ibrahim, Z.N. Rashid, L.M. Haji, N. Omar and H.I. Dino, Efficiency of semantic web implementation on cloud computing: A review, *Qubahan Academic Journal* **1**(3) (2021), 1–9.

[28] S. Aydin and M.N. Aydin, A sustainable multi-layered open data processing model for agriculture: Iot based case study using semantic web for hazelnut fields, *Adv. Sci. Technol. Eng. Syst. J* **5** (2020), 309–319.

[29] R. Afzaal and M. Shoaib, Data recoverability and estimation for perception layer in semantic web of things, *Plos one* **16**(2) (2021), e0245847.

[30] E. Kontopoulos, P. Mitzias, J. Moßgraber, P. Hertweck, H. van der Schaaf, D. Hilbring, F. Lombardo, D. Norbiato, M. Ferri, A. Karakostas et al., Ontology-based Representation of Crisis Management Procedures for Climate Events., in: *ISCRAM*, 2018.

[31] A. Chatzimichail, C. Chatzigeorgiou, A. Tsanousa, D. Ntioudis, G. Meditskos, F. Andritsopoulos, C. Karaberi, P. Kasnesis, D.G. Kogias, G. Gorgogetas et al., Internet of things infrastructure for security and safety in public places, *Information* **10**(11) (2019), 333.

[32] G. Bagschik, T. Menzel and M. Maurer, Ontology based scene creation for the development of automated vehicles, in: *2018 IEEE Intelligent Vehicles Symposium (IV)*, IEEE, 2018, pp. 1813–1820.

[33] H. Bista, I.-L. Yen, F. Bastani, M. Mueller and D. Moore, Semantic-based information sharing in vehicular networks, in: *2018 IEEE International Conference on Web Services (ICWS)*, IEEE, 2018, pp. 282–289.

[34] C. Choi and J. Choi, Ontology-based security context reasoning for power IoT-cloud security service, *IEEE Access* **7** (2019), 110510–110517.

[35] S. Alam, M.M. Chowdhury and J. Noll, Interoperability of security-enabled internet of things, *Wireless Personal Communications* **61** (2011), 567–586.

[36] 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* **78** (2018), 1040–1051.

[37] A. Ekelhart, S. Fenz and T. Neubauer, Aurum: A framework for information security risk management, in: *2009 42nd Hawaii International Conference on System Sciences*, IEEE, 2009, pp. 1–10.

[38] M. Välja, F. Heiding, U. Franke and R. Lagerström, Automating threat modeling using an ontology framework: Validated with data from critical infrastructures, *Cybersecurity* **3** (2020), 1–20.

[39] B.A. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins and R. Jardim-Goncalves, An ontology-based cybersecurity framework for the internet of things, *Sensors* **18**(9) (2018), 3053.

[40] 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)*, IEEE, 2015, pp. 1–6.

[41] M. Ficco, Security event correlation approach for cloud computing, *International Journal of High Performance Computing and Networking 1* **7**(3) (2013), 173–185.

[42] M. Ficco, L. Tasquier and R. Aversa, Intrusion detection in federated clouds, *International Journal of Computational Science and Engineering* **13**(3) (2016), 219–232.

[43] R. Syed, Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system, *Information & Management* **57**(6) (2020), 103334.

[44] J. Pastuszuk, P. Burek and B. Ksiezopolski, Cybersecurity ontology for dynamic analysis of IT systems, *Procedia Computer Science* **192** (2021), 1011–1020.

[45] A. Bryniarska, The auto-diagnosis of granulation of information retrieval on the web, *Algorithms* **13**(10) (2020), 264.

[46] A. Bryniarska, Certain information granule system as a result of sets approximation by fuzzy context, *International Journal of Approximate Reasoning* **111** (2019), 1–20.

[47] A. Bryniarska, Mathematical models of diagnostic information granules generated by scaling intuitionistic fuzzy sets, *Applied Sciences* **12**(5) (2022), 2597.

[48] Z. Xu, S. Zhang and Y. Dong, Mapping between relational database schema and OWL ontology for deep annotation, in: *2006 IEEE/WIC/ACM International Conference on Web Intelligence (WI 2006 Main Conference Proceedings)(WI'06)*, IEEE, 2006, pp. 548–552.

[49] M.A. Musen, The protégé project: a look back and a look forward, *AI matters* **1**(4) (2015), 4–12.

[50] B. Lantow, OntoMetrics: Putting Metrics into Use for Ontology Evaluation., in: *KEOD*, 2016, pp. 186–191.