An Ontology-based Security Framework for Decision-making in Industrial Systems

Bruno A. Mozzaquatro[1], Raquel Melo[2], Carlos Agostinho[2] and Ricardo Jardim-Goncalves[1]
[1]*Universidade Nova de Lisboa (UNL), DEE/FCT, 2829-516 Caparica, Portugal*
[2]*Centre of Technology and Systems, UNINOVA, 2829-516 Caparica, Portugal*

Keywords: Ontology, Internet of Things, Information Security, Decision-Making System, Adaptive Security.

Abstract: Embedded devices based on emerging technologies of the Internet of Things (IoT) are used to provide resources, business models and opportunities to build potential industrial systems improving manufacturing systems with efficient operations. In this context, IoT networks are dynamic environments and changes are also being increasingly frequent, modifying the environment execution. Nevertheless, severe threats will increase the complexity and difficulty to protect existing vulnerabilities in smart devices of IoT network. In this context, this work proposes an architecture of the ontology-based security framework to decision-making using adaptive security model to improve secure information for the industrial systems. IoTSec ontology contributes to feed the system using queries of contextual information collected in the environment. The main contribution of this approach is validated as an integration with C2NET project to ensure security properties in some critical scenarios.

1 INTRODUCTION

Smart devices integrated with different technologies allow several industrial applications with sensing, identification, localization, networking and processing capabilities. The information technology (IT) standards have beneficiated the industrial manufacturing by the evolution of industrial systems (Bi et al., 2014). The adoption of the Internet creates new business opportunities as well as exploiting collaborative work based on IT infrastructure in system environments. These aspects have potential to develop industrial systems like environmental monitoring, healthcare service, inventory and production management, food supply chain, transportation, workplace and home support, security and surveillance (Xu et al., 2014).

Heterogeneous environments with smart devices interconnected with the Internet increases the security threats. The main problem of IoT security is high interaction between humans, machines and IoT technologies with constraints in terms of connectivity, computational power and energy (Sicari et al., 2014). In contrast, severals security models, trust management, identity management and security mechanisms are used to ensure the privacy and security keeping security goals, such as: availability, confidentiality, integrity, authentication, non-repudiation, and authenticity (Roman et al., 2013) (Yan et al., 2014) (Granjal et al., 2014). Furthermore, IoT network is a dynamically changing environment and security issues require making-decision systems to change security mechanisms at run time (Evesti and Ovaska, 2013). Therefore, the adaptive security model is necessary to learn and adapt for adjusting on-demand security attributes and antecipates new threats in an information system (Habib and Leister, 2013).

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 (Yan et al., 2014). 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 (Mozzaquatro et al., 2015).

Model-Driven Development (MDD) has relevant aspects that contributes to develop adaptive systems considering adaptive model to monitor contextual information and take suitable actions at runtime (Soylu

Mozzaquatro, B., Melo, R., Agostinho, C. and Jardim-Goncalves, R.
An Ontology-based Security Framework for Decision-making in Industrial Systems.
DOI: 10.5220/0005853107790788
In *Proceedings of the 4th International Conference on Model-Driven Engineering and Software Development (MODELSWARD 2016)*, pages 779-788
ISBN: 978-989-758-168-7

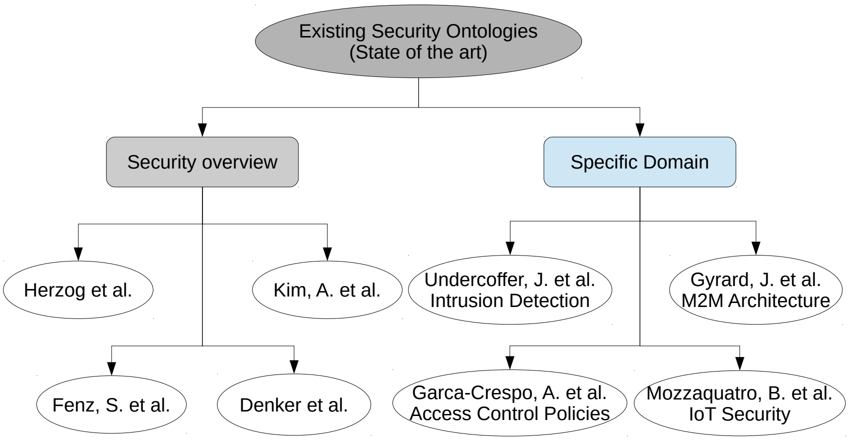

Figure 1: Existing security ontologies.

and De Causmaecker, 2009). In this context, the relation of MDD with Ontology Driven Development (ODD) employ the use of formal model to be employed at runtime. Hence, the application of ontologies for information security could improves real time detection of vulnerabilities, prediction and assessment of security risk management and intrusion detection (Undercoffer et al., 2003) (Xu et al., 2009) (Frye et al., 2012). Reference ontology in the security community has been identified as an important challenge (Mouratidis, 2006) and also for the Internet of Things. The previous work (Mozzaquatro et al., 2015) was proposed a reference ontology for security in the IoT with harmonization of existing security ontologies based on ontology development methodology. In addition, a security framework is fundamental to make secure the IoT environment allowing do queries and inferences to the security issues.

In this work we propose an architecture for an ontology-based adaptive security framework to identify common security issues using a knowledge base and demonstrate the contribution of application of the framework based on two security approaches: design and run time. This framework explores the knowledge base of IoTSec ontology (Mozzaquatro et al., 2015) to realize queries according to the contextual information collected of the smart environment in industrial scenario.

The rest of paper is organized as follow: Section 2 presents the background of security ontologies and adaptive security model. The related works are presented in Section 2.3. Section 4 describes the architecture proposed for ontology-based security framework. Section 5 describes a case study of the contribution of the approach. Finally, Section 6 presents the conclusion about this work.

2 BACKGROUND

This section describes main subjects involved in this work that contributes to improve the security aspects in the context of Internet of Things. In the following we discuss existing security ontologies (i.e. IoTSec ontology) and the adaptive security model to adapt mechanisms in a suitable solution. In addition, related works are presented to demonstrate the originality of the paper.

2.1 Security Ontologies

Security issues are important for all contexts with personal data exchanges and sensitive information, but for Internet of Things has important characteristics of a big concern with high iteration between humans, machines and IoT technologies. It is justified by heterogeneity of different smart devices connected with the Internet. In this context, ensuring security and privacy of applications and services is critical to improving trust and use of the Internet.

Therefore, these problems have potential because there are several situations of misunderstood concepts around information security and Internet of Things. For that, ontology is a potential tool largely utilized for structuring an area of interest.

According to the state of the art, several existing security ontologies have been proposed in the literature, but only a few are available (Figure 1): security overview ontology (Herzog et al., 2007) (Fenz and Ekelhart, 2009) (Kim et al., 2005) (Denker et al., 2003) and security ontology applied to specific domain (Undercoffer et al., 2003) (Gyrard et al., 2014) (García-Crespo et al., 2011) (Mozzaquatro et al., 2015).

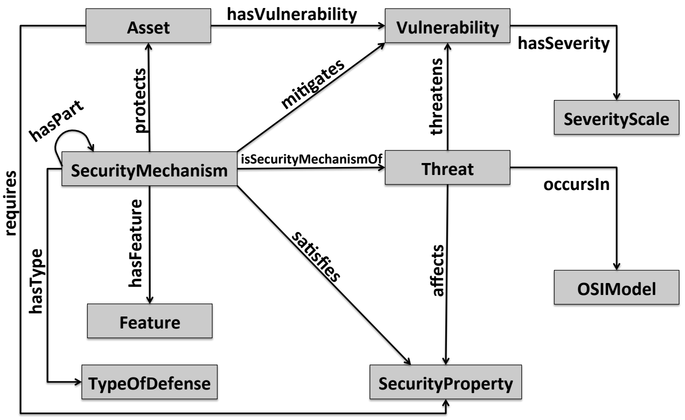

Figure 2: Reference ontology for security in IoT (Mozzaquatro et al., 2015).

Some ontologies address only one part of security domain (e.g. computer attacks) and others explore overview of information security. The previous work (Mozzaquatro et al., 2015) proposed a reference ontology for security in the IoT (IoTSec) with harmonization of ontologies based on ontology development methodology.

2.1.1 IoTSec Ontology

In this section, we describe the IoTSec ontology, which is a reference ontology for IoT security proposed in (Mozzaquatro et al., 2015). IoTSec ontology was proposed to explore aspects of relationships among basic components of the risk analysis of ISO/IEC 13335-1:2004 and National Institute of Standards and Technology (NIST) Special Publication 800-12 (Stoneburner et al., 2002) such as: Assets, Threats, SecurityMechanism, Vulnerability and Risk. Figure 2 presents an arrangement of top-level classes to modeling information security based in works (Herzog et al., 2007) (Fenz and Ekelhart, 2009) (Kim et al., 2005) (Denker et al., 2003) (Gyrard et al., 2014).

IoTSec ontology was designed based on information security issues that can be represents using a structured knowledge. Basically, ontology explores relationships among classic components of risk analysis to provide an overview of the domain of security in Internet of Things. IoTSec ontology was developed using the OWL (Web Ontology Language) ontology language.

These components allow to identify relations between relevant situations in an IoT network with risk analysis of potential threats. For example, the vulnerability class describes potential weakness of M2M technologies associated with Asset class (hasVulnerability property). In this ontology many technologies are considered assets such as: Wi-Fi, Web, GSM (2G), UTMS (3G), LTE (4G), Ethernet, Bluetooth, Sensor, etc. Assets require security properties to be considered secure such as availability, confidentiality, integrity, etc. Vulnerabilities are flaws in software or hardware and when they are discovered, vendors publish a patch to fix it. For instance, vulnerability notes database (VND)[1] is one example that provides information about software vulnerabilities including summaries, technical details, remediation information, and lists of affected vendors.

Meanwhile, security mechanisms are used to avoid that threats exploit vulnerabilities found. These mechanisms are categorized according to type of defense to protect the assets. A security mechanism is composed of several types of defense i.e., detective, preventive, corrective, recovery, response, etc.

Threat class describes information about attacks and others ways to exploit the applications' weakness and, sometimes, they explore one or more vulnerabilities. For instance, Wormhole attack replays messages from a system with the vulnerability of unprotected communication channel of a sensor network of an organization. This threat occurs in network layer of OSI Model (occursIn property). In this situation, SecurityMechanism class contains tools to protect using cryptography algorithms, but need to consider their strengths and weaknesses such as energy consumption, flexibility, high cost, etc.

Organizations may prevent exploitation of your vulnerabilities using security tools or algorithms to protect (mitigates property) the systems' weakness. Mitigates property represents the relationship between SecurityMechanism and Vulnerability class. Vulnerabilities are qualified in terms of your severity level (SeverityScale class) to an organization. Sometimes, organizations need to monitor the vulnerability with severity scale high, when systems have behavior

[1] http://nvd.nist.gov/

unpredictable and they can have become exposed to new threats. Each threat affects one or more security properties and the security mechanisms could satisfy these security properties.

2.2 Adaptive Security

Adaptive security is an approach to adjust attributes based on the behavior at runtime to respond for new and unusual threats in critical services (Abie, 2009) (Habib and Leister, 2013). This approach is found in the literature with concepts of self-adaptive software (Laddaga and Robertson, 2004) and autonomic computing (Dobson et al., 2006). It is a solution that learns and adapts to the changing environment at runtime in face of changing threats, and anticipates threats before they are manifested.

This approach is a continuous process to learn, adapt, prevent, identity and respond for unusual and malicious behavior in run time. For that, the adaptive security model proposed by (Shnitko, 2003) is composed by four components as depicted in Figure 3: monitor, analyzer, adapter, and adaptive knowledge database. The monitor collects attributes, analyzer determines the adaptation requirements, and adapter decides the adaptation plan for execution.

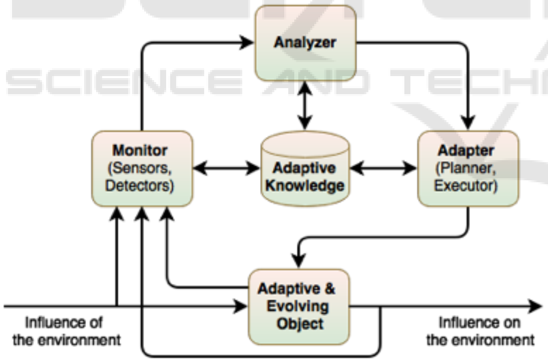
Analyzer
Monitor (Sensors, Detectors)
Adaptive Knowledge
Adapter (Planner, Executor)
Adaptive & Evolving Object
Influence of the environment
Influence on the environment

Figure 3: Adaptive and evolving security model (Shnitko, 2003).

The continuous cycle of security monitoring is needed for the use of suitable mechanisms depending of the information about the context and status of IoT devices. It is appropriated for IoT scenario because high interactions among heterogeneous devices and environment with critical risks to our lives. Monitoring information context allows to choose a suitable security tool for ensure one or more security properties. Sometimes, whether it changes the status of secure behavior of a given situation, the system need to change your rules to adapt and ensuring security properties.

According to (Habib and Leister, 2013) there is a little work on adaptive security mechanisms to secure IoT. Each work proposed explores platforms and specific aspects to improve IoT security as well as security policies, encryption, secure communication, and intrusion detection. Basically, there is a need for IoT security to adapt and adjust attributes when there is a change in the context. Nevertheless, the reliability and performance of adaptive security approaches is directly related with security mechanisms used to identify the threats in the system.

Within the scope of Model-Driven Development (MDD), adaptive security could be addressed to provides customization as a service in a runtime architecture. MDD is an approach composed by several theories and methodological frameworks for industrialized software development using models inside of software development cycle (Picek and Strahonja, 2007). There models and your transformations are described based on standard specification languages and generated automatically or semi-automatically from others abstract models. One relevant aspect of MDD to the adaptive security is the automation, which non-code artifacts are produced totally or partially from models (Picek and Strahonja, 2007) such as: documentation, test artifacts, build and deployment scripts and other models.

Adaptive actions are mediated by automated process through systems to maintain a formal model (i.e. context-aware) of the settings and relationships between them(Soylu and De Causmaecker, 2009). Besides it, model-driven approach can also be considered as an ontology driven approach, but the integration of these two approaches migh result benefits of inference support of ontological approaches and the expertise of model driven approach. Therefore adaptive actions are beneficiated with transformation of OWL/RDF knolwedge base into domain-centric data models (Kalyanpur et al., 2004).

2.3 Related Works

Ontologies has been explored in several aspects to improve information security, identifying vulnerabilities of systems, assessment the threat against targets using differents approaches, such as: intrusion detection (Undercoffer et al., 2003), correlation of context-aware alert analysis (Xu et al., 2009), identification of complex network attacks (Frye et al., 2012).

The work (Evesti and Ovaska, 2013) proposes an architectural approach for security adaptation in smart spaces utilized to analyzing and planning access control decision at runtime and design-time. The authors combines an adaptation loop of adaptive security model, Information Security Measuring Ontology (ISMO) to offer input knowledge for the adaption loop and a smart space security-control model to enforce dynamic access control policies. However, the work only illustrates the adaptive security approach from the authentication and authorization of users of smart spaces.

EDAS (Aman and Snekkenes, 2014) was proposed as an event driven adaptive security model to IoT to protect devices against threat faced at runtime. The authors use an Open Source Security Information Management (OSSIM) to filter and normalize events collected from *things*. They explore an Adaptation Ontology to leverages risks information from the event correlation and adapt security settings in terms of usability, QoS, and security reliability. However, the authors do not consider potential vulnerabilities that could prevent eventual threats in the environment. In this case, the approach need an occurrence to verify the suitable action to mitigate it.

In this context, this work explores a reference ontology for security in the Internet of Things. These knowledge based is composed by the basic components of risk management to ensure the secure environment with IoT devices. The relation between threat, vulnerability, asset, security mechanism and security property enable to make decision for use of potential solutions or identify weakness of products or softwares in industrial systems, for example. These ontology-based decision-making approach has potential to enrich security mechanisms of IoT devices network using adaptive security model through to respond for unusual behavior proposing other security tool or algorithms to protect assets.

3 C2NET PLATFORM

The C2NET platform is cloud-enabled tools for supporting collaborative demand to cover the supply networking optimization of manufacturing and logistic assets. The main problem of traditional supply chains has centralized decision-making approaches, which make difficult for companies to react to current highly dynamic markets. According it, C2NET platform is proposed to contributes in several aspects of industrial manufacturing exploring data collection of IoT devices in the companies' shop floor.

However, these devices are vulnerable for several threats and it needs to be addressed using security mechanisms. Moreover, some of these devices use different IoT technologies and C2NET platform explores the interoperability based on semantic web' technologies.

The C2NET architecture ensures interoperability by defining two components: C2NET Agent and C2NET Data Collection Client. Moreover, the C2NET platform has a module to collecting data from different sources and provide support for others modules of C2NET system.

3.1 C2NET Data Collection Client

The C2NET Data Collection Client (DCC) is a component of C2NET platform that provides the collecting and sending all the required data from the legacy systems of the company (e.g. its planning, logistics and operations) and data arriving from IoT devices in the shop floor (e.g. machine availability, performance, etc).

This component must be able to connect the different data sources (both legacy systems and IoT devices). Then, it will store the data gathered, and submit it to C2NET DCF as events when needed (both in a periodical basis or under demand). Consequently, the C2NET DCC will adopt an ESB pattern.

3.2 C2NET Agent

The C2NET Agent is a component of C2NET platform that receives the information generated in the platform (e.g. new collaborative production plans) for transferring it to the systems of the companies involved in the value chain. The C2NET platform will use the Agent API to communicate with the C2NET Agent, which exposes the legacy systems as business services. The C2NET Agent could receive the C2NET message and call the proprietary API of each legacy system to perform data update as needed.

3.3 C2NET Data Collection Framework

The C2NET Data Collection Framework (DCF) is a domain module that offers functionality for collecting data from different heterogeneous sources and providing necessary information for other modules of the C2NET system. This module enables uniform accessibility of structured information for data consumers. It also resolves challenges concerning integration and interoperability across data producers and consumers caused by differences in industrial processes, data models, methods, technologies and devices. It takes into consideration the homogenous integration of legacy systems and IoT devices.

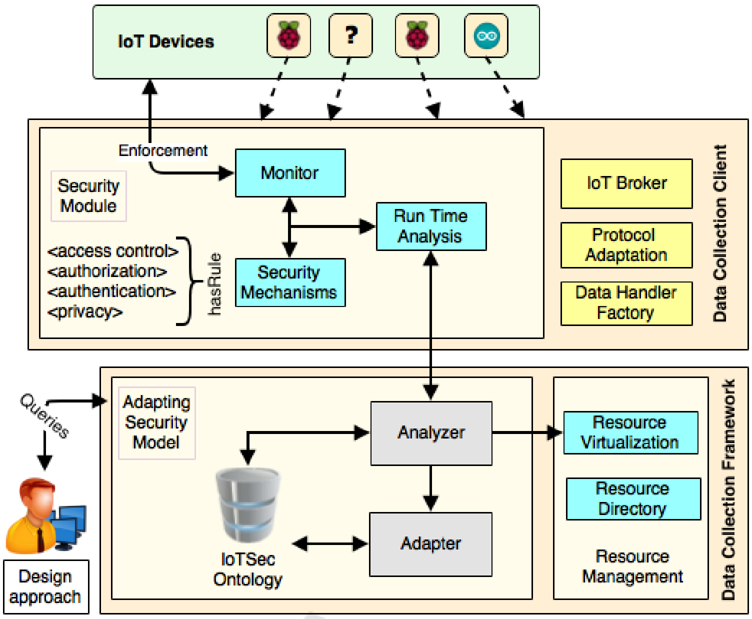

Figure 4: An architecture of ontology-based security framework proposed with the C2NET platform.

4 ONTOLOGY-BASED SECURITY FRAMEWORK

We develop our ontology-based security framework by following the adaptive security model presented in the Section 2.2. This type of security model is suitable for dynamic environment of Internet of Things, which monitor the behavior of the environment, learns and adapts for unusual occurences. In this context, the support of an adaptive knowledge base enables to antecipates threats before they are manifested in the IoT network.

Several industries are using of IoT devices to different applications to provides new opportunities based on sensing, ubiquitous identification, and communication capabilities (Xu et al., 2014). IoT devices transmit sensitive information of companies and they are vulnerable to internal and external attacks and appropriates actions need to be adopted to protect them.

The ontology-based security framework proposed in this work explores the adaptive security model to making-decision based on knowledge base for information security issues. For that, this security framework is integrated with the platform of C2NET project[2] to enrich security of IoT devices in industrial systems. In this context, the architecture of ontology-based security framework is depicted in the Figure 4. The architecture aims to improve security issues of industrial manufacturing integrated with the C2NET platform.

The C2NET platform uses IoT devices to data collect of the industrial environment using a company middleware with the C2NET Data Collection. Security mechanisms (i.e. based on rules, security protocols) are applied in data communication to protect sensitive information between IoT devices and middleware. Nevertheless, several vulnerabilities of devices and software appear everyday, which they becoming the assets vulnerable to attacks. Hence, continuous assessment and suitable adaptations need to be enforced to ensure the security properties such as availability, confidentiality, and integrity.

The security framework is proposed with two approaches to improve security issues of C2NET platform: design and run time. Design approach of the security framework explores the previous knowledge to adopt new technologies or products considering security issues. It has impact in the companies, because the responsible of purchases have not expertise in information security and it becomes the purchase of product without security analysis.

On the other hand, run time approach monitors IoT devices based on security metrics and attributes to identify malicious behaviors in the smart environment. Consequently, configurations and/or rules need to be adapted according the knowledge base, when alerts are triggered by security tools. For that, IoT ontology contributes to identify relations between threat, asset, vulnerability, security mechanism and security property. Nevertheless, the adapter infers in new

[2] http://c2net-project.eu

information on knowledge base to deploy new approaches for specifics situations or malicious behaviors.

Considering the approaches of security framework, this architecture is divided in two main components that are integrated with components of C2NET platform which are DCC and DCF. Design approach uses an interface to realize queries in C2NET DCF for data analysis based on the IoTSec ontology. This interface is used also to update the knowledge base when new information was published.

By other hand, the runtime approach has a Real Time Reasoning module to identify anomaly behaviour based on security mechanisms used in the environment. In this context, security attributes are monitored to detect malicious activities and, then, an action is trigerred to adjust settings using the adaptive security API of security framework.

4.1 Monitor Module

The Monitor module is responsible to data collection of information between IoT devices and enforce some suitable rules to the IoT newtork. These devices are used to information gathering of security attributes of environment. The monitor only considers device's information collected by devices to identify potential vulnerabilities that could be explored by the threats. Hence, raw data of the environment (e.g. shop floor) also is collected, but this information only is filtered by the platform to verify the proper operation based in the semantic of data.

This module uses a temporary set of security rules to apply of ensure a secure data communication between IoT devices. This approach is used in run time to make decision without delay. In this case, this set is feeded with previous knowledge of the ontology according to device's information of security attributes collected. For that, the Real Time Analysis module works together with monitor module to analyze parameters upward of threshold defined. For instance, any unusual behavior identified by security tools like intrusion detection system or firewall are fowarded to DCF component of C2NET platform to realize the most deep analysis of ontology-based security framework.

4.2 Analyzer Module

The Analyzer module of the security framework is responsible for consulting activities mapped in the knowledge base, but in case of new occurences (e.g. zero-day threats) reported by security tools, resulting in unusual behavior for the security framework. So, it needs to be adapted to avoid critical harms to the organizations.

DCF component of the C2NET platform manages the virtual instances of IoT devices to control your behavior in physical world. The Resource Virtualization is resposible to minimize the distance between physical devices and their virtualized devices in the IoT network. This information is important to analyzer module make decision for adaptation for potential security solutions between IoT devices.

4.3 Adapter Module

The Adapter module uses different adaptation methods to reconfiguration mechanisms employed by the adaptive security contained in the security framework. More information of this adaptation methods are found in (Elkhodary and Whittle, 2007).

5 ONTOLOGY-BASED SECURITY FRAMEWORK APPLICATION

In this section, we describe two validation scenarios of metalworking industry to apply the ontology-based security framework to improve the security issues between IoT devices and C2NET platform.

The IoTSec ontology was designed to allow decision-making following main classes of security: assets (K and X), vulnerabilities (Y), threats (Z), security mechanisms (G), and security properties. For instance, a sensor K (K requires some security properties J) based on technology X has vulnerabilities Y that can threatens by attack Z, but if the company use a security mechanism G, he could neutralize potential threats. Also, organizations need to define restrictions that can be represented by security policies and it means the security properties addressed for security framework.

To demontrate the application of security framework and relationship between IoTSec ontology and adaptive security model, Figure 5 presents a step-by-step application of framework.

- 1° step: The security attributes are collected by the environment to identify potential threats or security mechanisms to protect data communication, for example.
- 2° step: A temporary set of security rules is used to apply mechanism to protect devices and data transmissions. It is used for run time approach, which requires a fast decision-making based in previous knowledge.

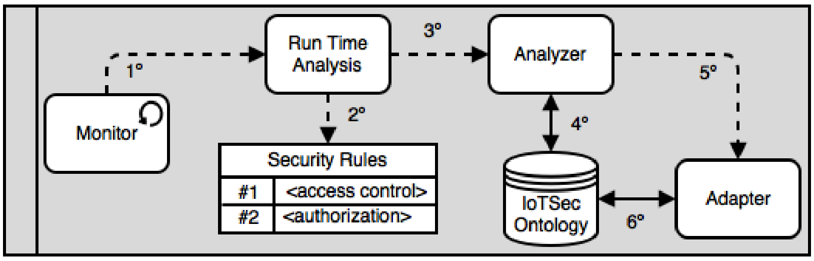

Figure 5: Step-by-step application of security framework.

- 3° step: In case of unusual behavior or a deep analysis is required to find other solutions. Thus, knowledge base is checked to identify suitable security mechanism that is related with a vulnerability.
- 4° step: SPARQL queries are used to collect information about an unusual behavior or a new vulnerability, for example. In this case, IoTSec ontology gives support for decision-making using security attributes collected by IoT devices.
- 5° step: Several situations are not mapped in knowledge base and it needs to be adapted using differents types of adaptation methods.
- 6° step: After a deep analysis the adaptation method update the knowledge base to future occurences.

We describe an overview of each scenario to understand the applicability of security framework and what information are important to monitoring for security level assessment. According to the restrictions and contextual information, security framework checks the knolwedge base using SPARQL Protocol and RDF Query Language (SPARQL)[3] queries and relates with others queries to identify suitable security mechanisms or potential threats, for example. Hence, in this work we considered that scenarios are vulnerable only for digital threats, such as disclosure information, replay attack, spoofing and others attacks to smart devices.

5.1 Collaborative Purchase

Collaborative purchase is a validation scenario that the C2NET platform allows to subscribe to common purchases on the same suppliers for the companies' partners. Collaborative purchase is need to found other companies that require same products of a specified supplier. Information of products that are missing are collected by using the IoT devices about the specifications and features of the raw material required (such as material type, material code, dimensions or weight), and also provides an expiration date for the same. This expiration date is related with the expected deadline for the purchase that is directly connected to the date that the company manager needs to have the product in his company. Moreover, smart sensors are used to verify the availability of the raw material and offer a collaborative purchase for others companies with the same supplier.

Metalworking industry imposes severe restrictions in the production process and one of them is the availability of raw material required to maintain it working. In this context, security property of availability of the sensors to gathering information about the products that are missing is fundamental to the process. The query following selects the security mechanisms that satisfies the security property "Availability". The variable ?secmech represents security mechanisms contained in the knowledge base and they are related with security property (variable ?secprop).

```
SELECT DISTINCT ?secmech ?secprop
WHERE
   ?secmech iotsec:satisfies ?secprop .
   ?secprop rdfs:label "Availability"@en
```

Moreover, authentication is another security property responsible to identify who has access to the information and avoid unauthorized user using these data. Sometimes, malicious employees or users using the Internet could explore vulnerabilities to realized attacks causing information disclosure or others critical consequences. For example, if a sensor has vulnerability that allows attackers get access of internal network it needs to be fixed. Hence, the ontology-based security framework has important role to check the relation between vulnerabilities and threats based on the knowledge base (IoTSec ontology). The query following uses the variable ?threat that threatens vulnerabilities selected by variable ?vuln.

```
SELECT DISTINCT ?threat ?vuln
WHERE
   ?threat rdfs:label ?label .
   ?threat iotsec:isVulnerabilityOf ?vuln
```

[3] http://www.w3.org/TR/rdf-sparql-query/

Security attributes of IoT devices the framework could suggest defense tools to block malicious behavior or attacks using prior knowledge. In another way, new activities are adapted with adjusting internal working parameters such as encryption schemes, algorithms of intrusion detection systems, different authentication and authorization mechanisms.

5.2 Non-conformity Scheduling

Non-conformity scheduling is a validation scenario composed of several IoT devices/sensors to feed the C2NET platform with real time detection of non-conformity products during the production process. It reduces the quantity of waste and non-conformity products that may arise during production process.

This scenario is the most critical in case of security issues because the C2NET platform collects information about the shop-floor production. Then, any violation in data communication between IoT devices and C2NET platform could compromise the production or to result critical problems to the company.

In this scenario the main security properties that need to be ensured are availability, integrity, confidentiality, and authentication. The availability property is recommended to maintain all information accessible to the C2NET platform as well as the continuity of production process. The integrity and confidentiality properties are two important aspects to avoid access to the information transmitted. For that, security framework contributes to choose suitable security tools with the relation between vulnerabilities, threats and security mechanisms. Basically, the query following shows how this information is obtained of IoTSec ontology, considering the variables `?threat`, `?secmec` (security mechanism) and `?secprop` (security property).

```
SELECT DISTINCT ?threat ?secmec ?secprop
WHERE
   ?threat rdfs:label ?label .
   ?threat iotsec:hasSecurityMechan ?secmec .
   ?secmec iotsec:satisfies ?secprop
```

In case of confidentiality, if an attacker has got access to the information transmitted, he can not understand this information because it must be encrypted. Moreover, the authentication property is related only with access control of the information by the C2NET platform.

6 CONCLUSION

We presented an architecture of ontology-based security framework to decision-making systems using adaptive security model to improve security issues in industrial scenario. In this context, the IoTSec ontology is responsible to shows a representation of structured knolwedge using semantic web technologies in the context of information security.

We have demonstrate how our proposed architecture ensure information security and there is potential to maintain security requirements need for risk management using main components of risk analysis. Merge between MDD and ODD approaches has potential to improve the reasoning and adaptive actions based on the knowledge base using contextual information.

After the integration of security framework with C2NET platform, we intend to continue checking new adaptive security models to replace or complement these already proposed; checking new knolwedge bases related of Internet of Things and M2M communication to specialize according to specific scenarios.

ACKNOWLEDGEMENTS

The research leading to this work has received funding from CAPES Proc. N^{o}: BEX 0966/15-0 and European Commission's Horizon 2020 Programme (H2020/2014-2020) under grant agreement: C2NET N^{o}: 636909.

REFERENCES

Abie, H. (2009). Adaptive security and trust management for autonomic message-oriented middleware. *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on*, pages 810–817.

Aman, W. and Snekkenes, E. (2014). Event driven adaptive security in internet of things. pages 7–15.

Bi, Z., Xu, L. D., and Wang, C. (2014). Internet of things for enterprise systems of modern manufacturing. *IEEE Transactions on Industrial Informatics*, 10(2):1537–1546.

Denker, G., Kagal, L., Finin, T., and Paolucci, M. (2003). Security for daml web services : Annotation and matchmaking. pages 335–350.

Dobson, S., Zambonelli, F., Denazis, S., Fernández, A., Ga"ıti, D., Gelenbe, E., Massacci, F., Nixon, P., Saffre, F., and Schmidt, N. (2006). A survey of autonomic communications. *ACM Transactions on Autonomous and Adaptive Systems*, 1(2):223–259.

Elkhodary, A. and Whittle, J. (2007). A survey of approaches to adaptive application security. In *Proceedings of the 2007 International Workshop on Software Engineering for Adaptive and Self-Managing Systems*, page 16. IEEE Computer Society.

Evesti, A. and Ovaska, E. (2013). Comparison of adaptive information security approaches. *ISRN Artificial Intelligence*, 2013.

Fenz, S. and Ekelhart, A. (2009). Formalizing information security knowledge. *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security - ASIACCS '09*, page 183.

Frye, L., Cheng, L., and Heflin, J. (2012). An ontology-based system to identify complex network attacks. *IEEE International Conference on Communications*, pages 6683–6688.

García-Crespo, Á., Gómez-Berbís, J. M., Colomo-Palacios, R., and Alor-Hernández, G. (2011). Securontology: A semantic web access control framework. *Computer Standards & Interfaces*, 33(1):42–49.

Granjal, J., Monteiro, E., and Silva, J. S. (2014). Security in the integration of low-power wireless sensor networks with the internet: A survey. *Ad Hoc Networks*, 24:264–287.

Gyrard, A., Bonnet, C., and Boudaoud, K. (2014). An ontology-based approach for helping to secure the etsi machine-to-machine architecture. *IEEE International Conference on Internet of Things 2014 (iThings)*.

Habib, K. and Leister, W. (2013). Adaptive security for the internet of things reference model. *Norsk informasjonssikkerhetskonferanse (NISK)*, pages 13–25.

Herzog, A., Shahmehri, N., and Duma, C. (2007). An ontology of information security. *Journal of Information Security*, 1(4):1–23.

Kalyanpur, A., Pastor, D. J., Battle, S., and Padget, J. A. (2004). Automatic mapping of owl ontologies into java. In *SEKE*, volume 4, pages 98–103. Citeseer.

Kim, A., Luo, J., and Kang, M. (2005). Security ontology for annotating resources. In *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE*, pages 1483–1499.

Laddaga, R. and Robertson, P. (2004). Self adaptive software : A position paper. *SELF-STAR: International Workshop on Self-* Properties in Complex Information Systems*, 19:31.

Mouratidis, H. (2006). *Integrating Security and Software Engineering: Advances and Future Visions: Advances and Future Visions*. IGI Global.

Mozzaquatro, B. A., Jardim-goncalves, R., and Agostinho, C. (2015). Towards a reference ontology for security in the internet of things. In *IEEE International Workshop on Measurement and Networking*, pages 1–6.

Picek, R. and Strahonja, V. (2007). Model driven development-future or failure of software development. In *IIS*, volume 7, pages 407–413.

Roman, R., Zhou, J., and Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10):2266–2279.

Shnitko, A. (2003). Adaptive security in complex information systems. In *Science and Technology, 2003. Proceedings KORUS 2003. The 7th Korea-Russia International Symposium on*, pages 206–210.

Sicari, S., Rizzardi, a., Grieco, L., and Coen-Porisini, a. (2014). Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, 76:146–164.

Soylu, A. and De Causmaecker, P. (2009). Merging model driven and ontology driven system development approaches pervasive computing perspective. In *Computer and Information Sciences, 2009. ISCIS 2009. 24th International Symposium on*, pages 730–735. IEEE.

Stoneburner, G., Goguen A. Y., and Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

Undercoffer, J., Joshi, A., and Pinkston, J. (2003). Modeling computer attacks : An ontology for intrusion detection. pages 113–135.

Xu, H., Xiao, D., and Wu, Z. (2009). Application of security ontology to context-aware alert analysis. *2009 Eighth IEEE/ACIS International Conference on Computer and Information Science*, pages 171–176.

Xu, L. D., He, W., and Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4):2233–2243.

Yan, Z., Zhang, P., and Vasilakos, A. V. (2014). A survey on trust management for internet of things. *Journal of Network and Computer Applications*, 42(2):120–134.