Towards Machine Learning Models as a Key Mean to Train and Optimize Multi-view Web Services Proxy Security Layer

https://doi.org/10.3991/ijes.v6i4.9883

Anass Misbah(✉), Ahmed Ettalbi
Mohammed V University, Rabat, Morocco
anassmisbah@gmail.com

Abstract—Muti-view Web services have brought many advantages regarding the early abstraction of end users needs and constraints. Thus, security has been positively impacted by this paradigm, particularly, within Web services applications area, and then Multi-view Web services.

In our previous work, we introduce the concept of Multi-view Web services to Internet of Things architecture within a Cloud infrastructure by proposing a Proxy Security Layer which consists of Multi-view Web services allowing the identification and categorizing of all interacting IoT objects and applications so as to increase the level of security and improve the control of transactions.

Besides, Artificial Intelligence and especially Machine Learning are growing fast and are making it possible to simulate human being intelligence in many domains; consequently, it is more and more possible to process automatically a large amount of data in order to make decision, bring new insights or even detect new threats / opportunities that we were not able to detect before by simple human means.

In this work, we are bringing together the power of the Machine Learning models and The Multi-view Web services Proxy Security Layer so as to verify permanently the consistency of the access rules, detect the suspicious intrusions, update the policy and also optimize the Multi-view Web services for a better performance of the whole Internet of Things architecture.

Keywords—Cyber Security, Internet of Things, Cloud, Multi-view Web services, Security layer, WADL, WSDL, Restful Architecture, Artificial Intelligence, Data science, Machine learning

1 Introduction

Multi-view Web services bring together the flexibility of Web services as well as user-oriented concept of the Multi-view abstraction notion. Therefore, in our previous works [1] and [2], we proposed a standardization and Restful implementation of Multi-view Web services. Moreover, in our work of [3] we came up with a new Layer (Proxy Security Layer) based on Multi-view Web Services in such manner to play a central role of communication control between IoT objects and applications within Cloud infrastructure.

In this work, we are moving forward, and improving the architecture of the Proxy Security Layer, through the integration of Machine Learning Models [15] as a key mean of training and optimizing the Multi-view Web services and then to make the Proxy Security Layer more accurate, self-updating and intelligent.

Indeed, the proposed architecture in our work of [3] injects a new Layer to secure transactions of IoT objects and applications within Cloud infrastructure, however, this layer is manually maintained, which is not practically possible especially when dealing with large amount of IoT objects and applications. Thus, came the motivation of this work, to address this issue by taking advantage of Artificial Intelligence and particularly Machine Learning Models in order to dynamically train and maintain the Proxy Security Layer.

In the following section, we discuss a brief technology over view as well as the state of the art of Machine Learning and Cyber security.

In section 3, we give a description of the problematic and also a detailed explanation of our contribution. Also in this section, we will highlight the main advantages of our contribution.

Afterwards, in section 4 we give a conclusion, before indicating some perspectives and future work in section 5.

2 State of the art

2.1 Multi-view Web services

The notion of Multi-view has been introduced in many previous works including [4]. This notion deals with end-users specificities at an early phase of conception especially with Object Oriented Modeling.

Hence, Multi-view allows making the abstraction level while modeling a system more efficient, less redundant and better secure. These improvements were possible through the injection of two main concepts:

View: Every atomic operation that can be done by one or multiple users (can be assumed to Web services methods)

Point of view: A set of views that can accessed by one or multiple users

Besides, the Multi-view concept was integrated with Web services in the work of [5] via the mechanism of the decomposition, the idea is to break down Web services to multiple Sub Web services (considered as views) and then generate for each user a set of Sub Web services according to his needs and access rights (considered as Point of view).

Moreover, an implementation of Multi-view Web services was proposed in the work of [6]. This implementation relays on an extension of the WSDL standard definition to a new derived definition called WSDL-Us.

Furthermore, in our work of [1], we went further and proposed a standard definition of Multi-view Web services that brings a new way of implementing Multi-view

Web services based on WSDL description format in addition to an automatic generation rules of this WSDL description.

Likewise, in our work of [2], we proposed another implementation of Multi-view Web services which is based on WADL description format so as to enlarge the integration possibilities of Multi-view Web services.

2.2 Internet of Things

Internet of Things (IoT) [7], can be considered as the evolution of the previous generation of connections between network nodes. In fact, IoT extend the notion of inter-connection to every object that is capable of sending or receiving a digital message. Objects can be devices, sensors, cars, home appliances, watches … and the messages can be used for state description, send instructions, alerts, monitoring…

The application of this communication architecture is really widespread among different kind of industries, and can bring a real business value when used in an efficient manner and setup with the right configuration.

Nevertheless, as articulated in [8], there is yet a lack of standardization in IoT area. In fact, IoT objects generally relay on manufacturer's standards and formats to exchange messages. Hence, there are still some challenges when it comes to security, performance and interoperability regarding IoT implementation.

In our work of [3], we also highlighted some security topics of IoT architecture that have been brought to the table by other works [12]. Such as Single Sign On, IoT networks analysis, IoT security common issues analysis and also a meta-model that propose security as a service (Secaas)

2.3 Cloud Computing

Cloud computing [10] is a custom service allowing organizations to get access to Infrastructure, Platforms, computation capacity or even Software without a long term investment. In fact, the outsourcing of such services makes it possible for companies (especially the ones that are not specialized in IT) to focus on their main business and let the service provider take care of all constraints related to infrastructure, platform and software maintenance and administration.

The infrastructure is hosted on the internet and maintained by the service provider as agreed upon the SLA (Service Level Agreements).

This concept brought many advantages regarding the scalability and flexibility of IT infrastructure, indeed, with Cloud computing it is possible to pay exactly what is consumed (cost optimization), to scale whenever needed (depending on business needs), to manage the whole platform remotely and also to delegate the security updates policy and compliance rules to the service provider (mutual costs).

Depending on the company's needs, the Cloud service can be (but not limited to):

Infrastructure as a Service (IaaS): In this kind of service, providing, the whole access is given to the customer to run and administrate the Infrastructure, this may include CPU, Memory, Hard Drive, and Operating System. Thus, the maintenance of the Infrastructure is carried by the customer.

Platform as a Service (PaaS): When allocating a platform as a service, the service provider should give access to an operational platform that the customer will use to set up his own software packages. The platform is maintained by the service provider; however, the software applications are taken in charge by the customer.

Software as a Service (SaaS): With software as service, the customer will have access to all needed applications without any effort of installation or maintenance, the whole software service is operated and guaranteed by the service provider, even the upgrade of software version. In this case, the software is ready to use and the customer just need to manage users and settings of the application.

Several works tackled the security within Cloud infrastructure, the work of [11] for example, proposed a solution by introducing the concept of Security as a Service (SecaaS), which consists of giving the customer the possibility to get access to pre-secured services, which means, the service consumer will no longer need to put in place and maintain any policy or rule of security since the security constraints are taken in charge in a centralized manner by the service provider.

Security of IoT objects within a Cloud infrastructure is also an important topic with many previous contributions and dedicated works, such as [9] that gave insights and examples of measures that can be put in place while setting up IoT architecture.

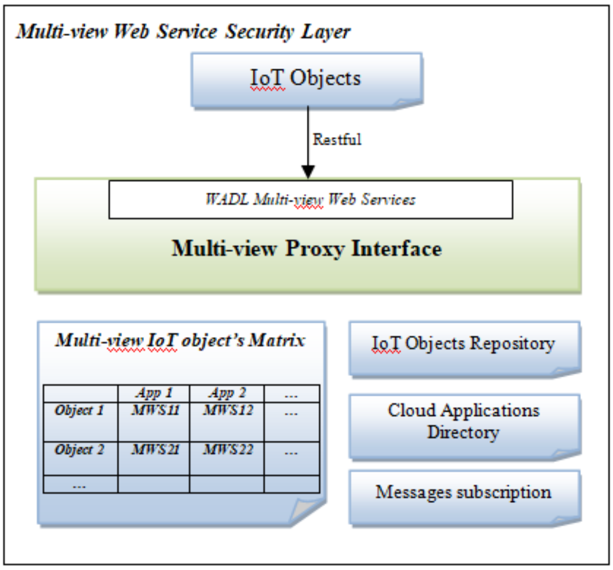
2.4 Proxy security Layer

Our work of [3] dealt with Multi-view Web services as a key component to build a new architecture layer (Proxy Security Layer) that provides a central control of the whole communications between IoT objects and applications within Cloud infrastructure. This control is achieved thanks to a User's Matrix table that contains all IoT objects (considered as Users) with the correspondent Point of view of each object (a set of views, each view is basically an application's operation). "Table 1" presents a reminder of the Muli-view Object's Matrix table defined in our work of [3].

Table 1. Multi-view Object's Matrix

IoT Objects	**Cloud Applications or objects**			
	Application 1	***Application 2***	***IoT object 6***	**…**
Object 1	MVWS 11	MVWS 12	xxx	…
Object 2	MVWS 21	MVWS 22	MVWS 26	…
…				

In addition, "Figure 1" presents an extract of the Proxy Security Layer architecture as described in our work of [3].


Multi-view Web Service Security Layer
IoT Objects
Restful
WADL Multi-view Web Services
Multi-view Proxy Interface
Multi-view IoT object's Matrix
IoT Objects Repository
Cloud Applications Directory
Messages subscription

	App 1	App 2	…
Object 1	MWS11	MWS12	…
Object 2	MWS21	MWS22	…
…			

Fig. 1. Architecture schema of the Multi-view Web service security Layer

2.5 Artificial Intelligence

Artificial Intelligence (AI) [13] is the science of imitating the human being cognitive intelligence in order to "learn" or "solve problems" as humans.

Over time, machines have became more and more "intelligent" which means capable of accomplishing tasks that were done only by Humans before, these tasks can be "manual" such as robotic industrial maneuvers, or "cognitive" such as image recognition, playing games or even self-driving cars.

In IT domain, the scope in which the machine has replaced the human is becoming larger and larger as the servers are becoming powerful and the algorithms more "intelligent" (can learn and solve problems).

Yet, there are still some frequent debates about what can be classified as AI or not, what can be done by machines or not, whether we can "trust" machines or not and if one day machines will reach the level of consciousness or not… Whatever answers would be, what we can actually notice for the time being is that machines are bringing a remarkable value in terms of Robotics, Learning and Natural Language Processing among others. Nevertheless, the work of AI still needs to be controlled (for instance we cannot rely on a medical diagnosis done by a machine without physician verification).

One of the most important items of Artificial Intelligence is the Machine Learning, in fact, the capacity of humans to learn is something that has amazed researchers' long time ago and has been a subject of lot of works and publications. Thus, lot of effort has been made to create algorithms capable of learning as humans from mistakes and reacting to the surrounding environment through discovery and adaptation faculty.

2.6 Machine Learning

Machine Learning [14] is the science of studying how machines can learn from experience such as humans.

This learning is realized thanks to statistical techniques and empirical data without a previous programming activity. In fact, unlike the programming science, Machine Learning deals with unknown results, in other words, Machine Learning helps figuring out new patterns, making predictions and also bringing new insights that we were not able to discover before by classical data analyze (Business Intelligence) and Data Mining techniques [18].

Among others, Machine Learning is used within IT organizations as a sub field of Data Analytics so as to find a new generation of solutions based on historical data.

This usage may be for inside IT maintenance (such as filtering E-mails, Intrusions detection, or computer vision) or to create Business value (such as predict the customer behavior, assess the Return on Investment, and evaluate an insurance product risk).

Machine Learning is operated mainly by dedicated contributors called Data Scientists; these contributors should have some important perquisites like:

- Mathematical and statistics background (Quantitative skills)
- Technical and Software programming aptitude
- Critical mind set, permanently questioning the results
- Curiosity and innovation thinking, “Think out of the box”
- Strong communication and Data representation skills

The Machine Learning tasks can be operated with predefined labels (list of classification categories that the results should fall into) and possibly, with “feedbacks” or “indicators” to drive the learning process; in this case we are talking about Supervised Learning. Or, without any clue about what the result can look like, in this case we are talking about Unsupervised Learning. This second category of Machine Learning is used to discover hidden patterns in Data or explain a strange phenomenon.

Supervised Learning: Supervised Learning [15] relays mainly on the notion of “training data”, this data is composed of historical examples and consists of (inputs, outputs) vectors that will be used to build a new inference function. This inference function is utilized to predict outputs depending on the inputs (automatic mapping of inputs - outputs).

This learning process can be refined continuously through new examples and feedbacks that contribute to the re-adaptation of the inference function. Then, the results can be controlled and the accuracy of the inference function can be assessed.

One main concept to take under consideration when carrying Supervised Learning and Machine Learning in general is that the results strongly depend on the amount of injected data. In fact, the more data we inject to the machine the more accurate the result will be.

One good practice also in this category of learning is to train the model with only 80% of data (training data), and leave the 20% for validation purposes (Validation data). Indeed, since we have the inputs – outputs of the remaining 20% validation data, we will be able to verify the accuracy of the results and then to assess the relevance of the chosen model.

As the use cases of unsupervised Machine Learning, the expected outputs and also the nature of data can vary, then the choice of the appropriate model can also vary depending on the case. That is why we usually do not use one model to build the inference function, but we apply multiple models so as to choose the more suitable at the end (with the higher accuracy rate).

The most commonly used Supervised Learning algorithms are:

- Support Vector Machines
- Linear regression
- Logistic regression
- Naive Bayes
- Linear discriminant analysis
- Decision trees
- K-nearest neighbor algorithm
- Neural Networks (Multilayer perceptron)

Since the scope of this work do not include the implementation of one particular algorithm, we will not go further in the description of these models. Instead, we will focus on how to bring the power of Machine Learning together with the flexibility of Multi-view Web services to inject an “Artificial Intelligence” within the Proxy Security Layer.

Unsupervised Learning: Contrary to Supervised Learning, with Unsupervised Learning [16] there are no initial labels or [inputs – outputs] examples. The classification is applied to the learning data and the outputs are usually unexpected patterns and models.

In this case of Unsupervised Learning, there is no precise way to verify the accuracy of the model, it is left to the experts’ appreciation to confirm or invalidate the results.

Unsupervised Learning can be grouped mainly to two groups:

- Clustering: This type of models is used to group some type of data fields by the same characteristics or behaviors (such as grouping students having the same social habits)
- Association rules: This kind of algorithms can be used to discover some hidden associations in the data (such as students subscribed to the course A would also be interested in course B)

Some examples of algorithms used in Unsupervised Learning are the following:

- Clustering
- Anomaly detection

- Neural Networks

Reinforcement Learning: Reinforcement Learning [17] is characterized by the concept of "feedback". This feedback can be a reward or a punishment depending on the interpretation of the system. In fact, the agent (which is the Machine Learning algorithm actually) take actions in a given environment, and is provided with a feedback and a new state of the environment. Hence, the agent is built in such manner to learn permanently a new way to take actions that will maximize the reward and minimize the punishment as well as maintaining the environment in a stable condition.

This Machine Learning category is not about a concrete inputs – outputs as Supervised Learning, instead, it is about improving permanently the results through experience and then gain strong skills regarding the given environment.

Additionally, the application domains of Reinforcement Learning are numerous and can vary among resources management and planning, traffic control, robotics, Chemistry, marketing, advertising and also games. As an example, one of the most important achievements of Reinforcement Learning is the computer program AlphaGo developed by Google DeepMind [20] beating Lee Sedol with the final score of 4 – 1 in the favor of AlphaGo.

2.7 Machine Learning in Cyber Security

Machine Learning has been introduced in many previous works as a key support mean of traditional IDS (Intrusion Detection Systems) solutions to update IT security policies, and discover a new patterns of cyber attacks.

The work of [18] consists of a survey of Data Mining and Machine Learning methods for Cyber Security Intrusion Detection. This work focus on some examples within the state of the art of existing Machine Learning and Data Mining methods that are used to support the IDS for a better and more efficient intrusion detection.

This same work [18] summarized some selected use cases of each method and described the correspondent Cyber Data sets. In addition, a comparison of implementation complexities and challenges is addressed and discussed.

However, this work relays only on existing researches, and do not bring a new contribution to enrich the scope of Machine Learning application within the field of Cyber Security.

Besides, the contribution of [19] gave an overview of cyber-attacks vulnerabilities as well as some Machine Learning methods used to set up more reliable cyber-defense systems. Afterward, in the work of [19] there is also a description of some specific cyber-security problems (misuse detection, anomaly detection, intrusion detection, scan detection, profiling network traffic, privacy preserving) with related Machine Learning solutions as well as a discussion about challenges and difficulties with each method.

Eventually, in [19] there is also a discussion about emergent cyber attacks and some research axes regarding the cyber defense strategies that can be put in place to face this threats (which can be considered as a research area to cover in the near future).

3 Our contribution

3.1 Problematic

In our previous work [3] we proposed a Proxy Security Layer which is responsible of controlling and securing the communications within IoT architecture. This control is achieved among others thanks to the Multi-view Objects matrix table that contains all IoT objects and applications (Users, Points of view and Views)

This table is given a central role within the architecture, and even though the WADL definition of Multi-view Web services is generated dynamically as proposed in our previous work, the identification, categorizing and optimization of these Multi-view Web services are done manually. Hence, in a large architecture with huge amount of IoT objects and applications, it will be laborious or even impossible to manually establish, maintain and optimize this Multi-view Objects matrix table

Therefore, in this work, we are coming up with a new solution to this issue by introducing the concept of Machine Learning as a key element of the Multi-view Objects matrix table continuous improvement. This improvement can be reached via self trained models that are capable of proposing new classification (the correspondence between IoT objects and applications, can also be seen as access rules) in a supervised system (The classes are given prior to the model predictions, then each prediction should fall into a predefined class) or find a way to optimize and maintain the current classification in an unsupervised system (the model can predict new classes, which means we will be able to predict a new type of access rules)

This amelioration will make the whole architecture more robust and sustainable. In the next section we are giving more details about this proposed approach.

3.2 Proposed solution

The value proposition of this work is articulated mainly in these areas:

Supervised Learning: The system makes propositions of a new classification based on the historical data. In this case we can think of the new classification as the set of new Multi-view Web services and sub Web services with predicted access rules to some IoT objects or applications.

In supervised learning the system will be given the classes that we are trying to classify into (for example a new Point of View and the related Views, which means the Multi-view Web services and Sub Web services)

The following schema (Figure 2) illustrate the inputs and outputs of this category of Machine Learning

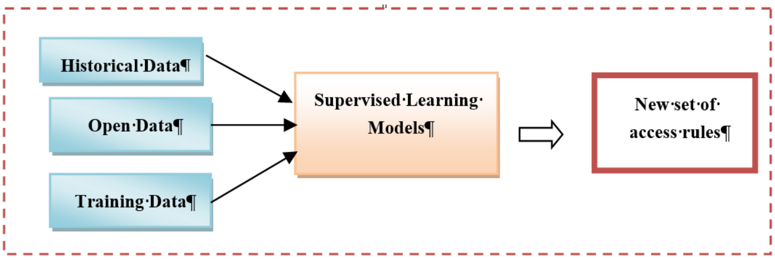


Fig. 2. Inputs and Outputs of Supervised Learning Models

Historical Data: This part can be relatively huge depending on the depth of Data captured regarding the previous events of IoT objects accessing to applications or to other IoT objects. It is important to note that IoT objects can generate very quickly a large amount of data that cannot be processed manually. And there came the need to store and process this Data using Big Data technologies and Machine Learning algorithms to get new insights from this Data.

Open Data: This Data can be found publically and used for free without any constraints. Usually we make use of this Data when we do not have enough Data locally to give consistent predictions. Indeed, the more historical Data we have the best and accurate the predictions will be. In addition, this Data must be provided by an organization within the same industry and operations domain, in fact, heterogeneous Business domains can result to an incoherent predictions.

Training Data: Training Data is given as a teaching set of Data that is provided as examples. Again, the more sample examples are given the best results we will get. In our case, we can give some examples about access rights concerning some IoT objects and applications.

Supervised Learning Models: The supervised Learning algorithms are multiple (as detailed previously) and can be implemented differently depending on the context (labels, variables, outputs, hyper parameters, Data…). In this work we do not deal with the implementation of a specific algorithm, instead we propose a meta model that rely on these algorithms to predict a new set of access rules (as shown in figure 2)

The Supervised Learning Models will take into consideration all provided Data (Open Data, Training Data, and Historical Data) while running the selected algorithm with the defined parameters and then predict a new set of access rules. In our case the new set of access rules will be the Points of view and Views for each user (Cloud Applications and sub applications for each IoT object)

As Supervised Learning algorithms are based on predefined classes, in our case the classes correspond to the set of predefined IoT objects and the Cloud applications (Users and Points of view)

This prediction will make it possible to insert automatically new rules to the Multi-view Objects matrix table as well as confirm or not the validity of the existing rules.

New set of access rules: This new set is basically the update of the Multi-view Objects matrix table that will propose new entries to this table or update the existing ones.

Reinforcement Learning: This Learning method is based on Reward / Punishment feedback, in our case it can be used a posteriori after a classification by giving some feedback from agents (human or robot) regarding the prediction so as the model is improved permanently through feedbacks

In the case of Proxy Security Layer, this method can be implemented by using an initial set of access rules, run the model to make the predictions and then check the results manually or automatically so that the model is updated accordingly

The following schema (Figure 3) illustrate the inputs and outputs of this category of Machine Learning

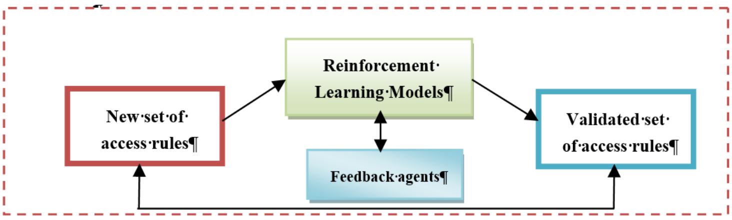

Reinforcement·Learning·Models¶
New·set·of·access·rules¶
Validated·set·of·access·rules¶
Feedback·agents¶

Fig. 3. Inputs and Outputs of Reinforcement Learning Models

New set of access rules: This new set can be the result of a previous Supervised Learning phase or any initial set of rules stated in the Multi-view Objects matrix table

Reinforcement Learning Models: Unlike the Supervised Learning, Reinforcement learning is concerned with the existence of an optimal solution. Thus, this method relies on continuous improvement process within a given environment. This improvement can be reached through a loop of feedbacks that the model get from agents by means of rewards / punishments depending on the prediction accuracy

In our case, the environment will be the New set of access rules, and the agents can be human (system administrators, cyber security mediators…), robots (expert systems, automates) or both; the validated set of access rules will be updated and improved continuously according to the agents feedback.

Validated set of access rules: Since the Reinforcement Learning is a continuous process, each time we are applying Reinforcement learning models and taking under consideration the feedback from agents to set a new improved access rules list. This same improved list will be used as an environment to improve the access rules again and again in the Reinforcement process. The result of this process is the optimization and reliability of the Multi-view Objects matrix table, as well as the detection of abnormal activities which can help detect intrusions and breaches.

Generally, in this kind of Machine Learning models, the target is to reach a better prediction each time; it is used when we are not looking for the best solution, but a better solution that can be improved through agent’s feedback and experience

Unsupervised Learning: This Machine learning category deals with unknown patterns and Data classification, in fact, unlike Supervised Learning, Unsupervised Learning models try to figure out new classes (also called labels) automatically. In other words, we will start from a set of Data and then apply the Unsupervised Learning inference algorithms to find patterns and classes. These classes will make it possible to predict for future Data which pattern it matches, and subsequently predict the related characteristics accordingly

Regarding the case of Multi-view Object's Matrix table, the Unsupervised Learning can take as an input the validated set of access rules then apply inference algorithms of Unsupervised Learning so as to figure out new classes. These classes represent the new patterns of IoT objects and Points of view. Therefore, this inference will help defining new categories of access rules that was not visible before in addition to optimizing the current access rules (for instance, when having lot of access rules with the same characteristics that are materialized by separated classes, Unsupervised Learning will bring a new class replacing the old classes. This substitution is possible as long as these classes have all the same behaviors statistically and then can be grouped to a unique class). As a result we will have an optimized set of access rules as shown in (figure 4)

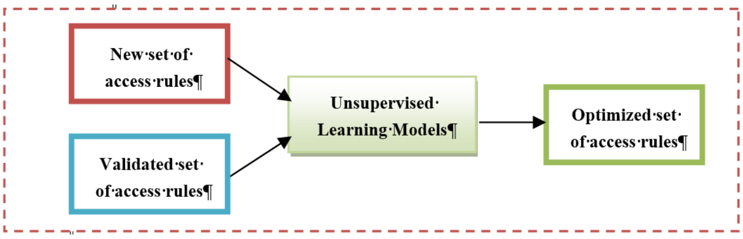


Fig. 4. Inputs and Outputs of Unsupervised Learning Models

Unsupervised Learning Models: These Learning algorithms will take as inputs the Multi-view Objects Matrix table which consists of a new set of access rules and / or a validated set of access rules. Then apply inference algorithms so as to predict new patterns of Points of view and Users (Cloud applications and IoT Objects). These patterns will define the new optimized set of access rules

It is to consider that the predicted patterns are not always applicable, in fact, sometimes some predicted patterns do not correspond to a valid set of access rules regarding the actual context, in this particular case, these patterns shall not be considered

Optimized set of access rules: This new set of access rules will be defined via new predicted patterns that will be used either to summarize the same kind of access rules into a unique access rule or to bring new classes that were not visible before (for instance in case of a possible communication between an IoT object and an application that was not identified before because it has never happened).

3.3 Advantages of the proposed approach

In this work, we continue developing our previous works by injecting Artificial Intelligence within the Proxy Security Layer. Thus we combined all advantages of Multi-view Web services and Machine Learning so as to build a strong meta-model capable of handling security issues concerning IoT communication within a Cloud infrastructure.

Therefore, many advantages can be noticed regarding our contribution, among others, we highlight the followings:

- Addressing one of the most challenging subjects which is the Cyber Security of IoT devices within Cloud infrastructure
- Enhancing security with IoT objects will lead to more application areas and then promote the usage of IoT among different industries
- Bringing advantages of Multi-view Web services (Flexibility, Standard, restful, optimization, easy-to-use, self-validated, interoperability and automatic generation)
- Injecting Artificial Intelligence allows to implement the Proxy Security Layer within large environments with huge amount of IoT objects since the data is treated dynamically by agents
- Combining the three categories of Machine Learning (Supervised, Unsupervised and Reinforcement Learning) bring a powerful set of models that can be implemented with different contexts and then cover a large amount of Cyber security concerns
- Machine Learning allow to learn from experience, discover a new patterns and also figure out a new classifications, therefore, when bringing these elements to Cyber security, the defense strategy approach is more proactive than reactive. In fact, unlike the classical IDS (Intrusion Detection Systems) IPS (Intrusion Prevention Systems) with reactive detection, our approach is proactive based, since it is possible to discover a breach before it happened and also predict vulnerabilities
- The growing fast community of Data Scientists is updating permanently the Machine Learning algorithms and the public open data, consequently, the predicted data will be more and more accurate and relevant
- As Big Data tools handle “structured” and “unstructured” data, it will be possible to explore a larger amount of data entries while making predictions and therefore figure out more accurate results

4 Conclusion

This work proposed a high level architecture of a Proxy Security Layer that takes advantages of Multi-view Web services properties as well as the intelligence of Machine Learning models.

The idea behind our work is not to deal with a specific implementation of a Machine Learning algorithm in a given IoT – Cloud environment. Instead, our work is about to handle every kind of IoT environment by proposing a high level architecture that can be declined differently depending on implementation environment.

The implementation of this architecture should take under consideration many parameters such as: The environment cyber attacks vulnerabilities, the available historical data, the confidentiality of transactions, the volume of IoT equipments, the tolerance level that we are willing to accept, and the available computational power …

Eventually, the implementation will not be about a best model to adopt, but about an initial most accurate model that we will improve over time through experience and feedback.

5 Perspectives and Future work

As future work, we will continue exploring the application areas of Muti-view Web services so as to create added value in different IT fields by means of the flexibility, standardization, automation and also easy-to-implement of Multi-view Web service.

Moreover, there are some fields to be studied regarding Machine Learning and the solutions that they can bring to address Cyber security issues.

Finally, the implementation possibilities can be an interesting zone to cover in order to come up with specific solution to a given problem.

6 References

[1] Misbah, A., Ettalbi, A.: Towards a standard WSDL implementation of Multiview web services. In: 5th International Conference on Multimedia Computing and Systems (ICMCS'16) – IEEE Conference, 29 September – 1 October (2016), Marrakech, Morocco. https://doi.org/10.1109/ICMCS.2016.7905542

[2] Misbah, A., Ettalbi, A.: Towards a standard Restful WADL implementation of Multiview, web services. IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.4, pp. 315-320, April 2017

[3] Misbah, A., Ettalbi, A. Multi-view Web services as a key security layer in Internet of Things architecture within a Cloud infrastructure. 13th International Conference on Information Assurance and Security (IAS 2017) – 11-13 December (2017), Marrakech, Morocco.

[4] Kriouile, A.: VBOOM, Object-oriented analysis and design method by points of view, PhD thesis. Mohammed V University. Rabat, Morocco. (1995)

[5] Boukour, R., Ettalbi, A. and Nassar, M.: Multiview Web Service: The Integration of The Notion of View And Point of View in The Web Services. International Journal of Computer Science and Network Security (IJCSNS), vol. 14 no.2, pp. 31-36, February (2014)

[6] Boukour, R., Ettalbi, A. and Nassar, M.: Multiview web service: The description Multiview WSDL of Web Services. In: International Symposium on Signal, Image, Video and Communications (ISIVC'2014), November 19-21, (2014), Marrakech, Morocco.

[7] Vermesan, Ovidiu; Friess, Peter (2013). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. Aalborg, Denmark: River Publishers. ISBN 978-87-92982-96-4.

[8] Wood, Alex (31 March 2015). "The internet of things is revolutionizing our lives, but standards are a must". The Guardian.

[9] Singh, Jatinder; Pasquier, Thomas; Bacon, Jean; Ko, Hajoon; Eyers, David (2015). "Twenty Cloud Security Considerations for Supporting the Internet of Things". IEEE Internet of Things Journal. 3 (3): 1. https://doi.org/10.1109/JIOT.2015.2460333

[10] Hassan, Qusay (2011). "Demystifying Cloud Computing". The Journal of Defense Software Engineering. CrossTalk. 2011 (Jan/Feb): 16–21. Retrieved 11 December 2014.

[11] Furfaro, A.; Garro, A.; Tundis, A. (2014-10-01). "Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing". 2014 International Carnahan Conference on Security Technology (ICCST): 1–6. https://doi.org/10.1109/CCST.2014.6986995

[12] Qi Jing; Athanasios V. Vasilakos; Jiafu Wan; Jingwei Lu; Dechao Qiu. "Security of the Internet of Things: perspectives and challenges". Wireless Netw DOI 10.1007/s11276-014-0761-7 https://doi.org/10.1007/s11276-014-0761-7

[13] Rubin, Charles (Spring 2003). "Artificial Intelligence and Human Nature |`The New Atlantis". 1: 88–100. Archived from the original on 11 June 2012.

[14] Alpaydin, Ethem (2010). Introduction to Machine Learning. London: The MIT Press. ISBN 978-0-262-01243-0. Retrieved 4 February 2017

[15] Mehryar Mohri, Afshin Rostamizadeh, Ameet Talwalkar (2012) Foundations of Machine Learning, The MIT Press ISBN 9780262018258.

[16] Duda, Richard O.; Hart, Peter E.; Stork, David G. (2001). "Unsupervised Learning and Clustering". Pattern classification (2nd ed.). Wiley. ISBN 0-471-05669-3

[17] Sutton, Richard S.; Barto, Andrew G. (1998). Reinforcement Learning: An Introduction. MIT Press. ISBN 0-262-19398-1.

[18] Anna L. Buczak, Erhan Guven.: A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 2, SECOND QUARTER 2016

[19] Sumeet Dua, Xian Du.: Data Mining and Machine Learning in Cybersecurity. Auerbach Publications Taylor & Francis Group 2011. https://doi.org/10.1201/b10867

[20] "Artificial intelligence: Google's AlphaGo beats Go master Lee Se-dol". BBC News. Retrieved 17 March 2016.

[21] Misbah, A., Ettalbi, A. Automatic conversion of a Conceptual Model to a Standard Multi-view Web services definition. iJES International Journal of Recent Contributions from Engineering, Science & IT, VOL.6 No.1, pp. 43-56, 2018.

7 Authors

Anass Misbah is PhD student at IMS Team, ADMIR Laboratory, ENSIAS, Rabat IT Center, Morocco.

Ahmed Ettalbi is Professor at Software Engineering Department of the Higher National School of Computer Science and Systems Analysis (ENSIAS) Rabat, Morocco. His main research interests Object Modeling with Viewpoints, Software Architecture and Business Process Modeling architecture.

Article submitted 09 November 2018. Resubmitted 22 November 2018. Final acceptance 25 November 2018. Final version published as submitted by the authors.