Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things

Aissam OUTCHAKOUCHT
PhD Student, Laboratory LISER
IPI, Paris, France

Hamza ES-SAMAALI
PhD Student, Laboratory LISER
IPI, Paris, France

Jean Philippe LEROY
Laboratory LISER
IPI, Paris, France

***Abstract*—The Internet of Things (IoT) is now destroying the barriers between the real and digital worlds. However, one of the huge problems that can slow down the development of this global wave, or even stop it, concerns security and privacy requirements. The criticality of these latter comes especially from the fact that the smart objects may contain very intimate information or even may be responsible for protecting people's lives. In this paper, the focus is on access control in the IoT context by proposing a dynamic and fully distributed security policy. Our proposal will be based, on one hand, on the concept of the blockchain to ensure the distributed aspect strongly recommended in the IoT; and on the other hand on machine learning algorithms, particularly on reinforcement learning category, in order to provide a dynamic, optimized and self-adjusted security policy.**

***Keywords*—Internet of Things; security; access control; dynamic policy; security policy; blockchain; machine learning; reinforcement learning**

I. INTRODUCTION

Several works have dealt with the access control (AC) in the literature. Meanwhile, in constrained environments as the case in IoT, those concerns are not yet mature enough. This section is about introducing the IoT paradigm, basically from an AC point of view, and then will present how security policies are managed in the existing AC models.

A. Internet of things paradigm

The Internet of things (IoT) is now a reality that surrounds us covering several parts of our lives, and will become more so in the future. Indeed, many researches consider IoT as one of the main technological revolutions of this century [1] and have moved from being a futuristic vision to an increasing market and research reality. It was in 2008 that the world passed the barrier of a single connected object per person and the statistics are now talking about numbers around 26 smart objects for every human being on earth by 2020 [2].

However, the Internet of Things, and despite all what has been said, is still maturing, in particular due to numerous challenges which slow down the full exploitation of the IoT, namely the computation constraints of the IoT devices, heterogeneity, identification, power supply, data storage/processing, etc. Meanwhile, one of the most crucial of these challenges concerns security and privacy, especially given the ubiquity of the smart objects in every corner of human life.

Unfortunately, what makes things worse; the traditional security solutions are not applicable in general in the context of IoT environments given the constraints of the IoT components which are characterized by low capabilities in terms of both energy and computing resources and thus, they cannot implement complex schemes supporting security. The OWASP Internet of Things Project has listed the most common IoT attacks and vulnerabilities [3]. According to this project, the risk arises because of the lack of adoption of well-known security techniques, such as encryption, authentication, access control and role-based access control. A reason for this lack of adoption is that existing security techniques, tools, and products may not be easily applied to IoT devices and systems.

To mitigate these risks, the deployed IoT services have to be "smart" and function in an open, dynamic and completely distributed environment. This requires that they gain a greater degree of autonomy and decision making.

B. IoT and Access control

Authentication and access control technologies are known as the main elements to address the security issues in the Internet of Things. Actually, any effective access control system should satisfy the main security properties of the CIA triad: Confidentiality, integrity and availability. Note that one should not confuse AC with identification and authentication notions. Fig. 1 shows the boundaries of the access control process.

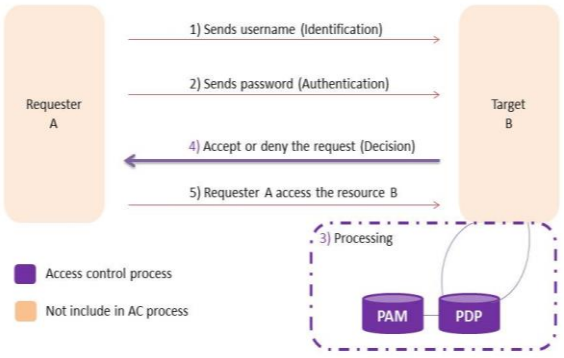

Fig. 1. Boundaries of access control.

Many access control models have been proposed in the literature to address security issues in IoT, but almost all of them are based on a centralized architecture, static security policy whose limitations in IoT context will be explained later.

As in the case of security mechanisms in general, applying current access control solutions on the device's side is not trivial. It requires intensive and computational capabilities which are not available in the most used IoT constrained devices. However, outsourcing the management of access control to non-constrained nodes presents serious security and privacy problems (e.g. break end-to-end security) and necessitates a high level of trust between the stakeholders. Furthermore, all interactions between them must be secured and mutually authenticated. To remedy what we have just cited, IoT needs an access control framework suitable to its distributed nature, where users may control their own privacy and, rather than being controlled by a centralized authority, and at the same time, the need arise for centralized entity handling authorization function to hardly constrained IoT devices.

C. Security policy management

The Common Criteria defines an organizational security policy as: a set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment [4].

Access-control policies have developed from trivial matrices to extremely complex representation expressed in sophisticated and advanced languages. It is then clear that this expansion and complexity require consequently robust automatic techniques to understand and manage them [5].

In traditional access control models access control policies are a set of rules stored somewhere in a server or, at best, distributed on several nodes in the network. In the case of the internet of the things it is necessary to have, in one hand a distributed policy that goes with the decentralized aspect of IoT and that is why (and for other reasons detailed later) we have chosen the blockchain technology as the basis of the proposed framework, and in the other hand a dynamic policy which takes into consideration the context in which the smart devices are, but also which can be improved over time, this improvement obviously does not, and cannot, be managed by a human being given the enormous and heterogeneous amount of data that the IoT generates. We therefore think in this paper to use the power of artificial intelligence algorithms, especially those of machine learning, to ensure this task.

II. BACKGROUND

This section gives an overview of the basic concepts necessary to understand the proposed framework whether in terms of architecture or functioning.

A. IoT and Machine learning algorithms

The internet of things is basically composed of various self-directed and low power devices. These nodes are able to collect information about their entourage with sensors, act on that environment (by using actuators) and communicate with each other and even with other entities like the Cloud.

The concept of machine learning (ML) was first treated as an artificial intelligence (AI) technique [6] then focused more and more in the complex algorithms that are difficult to manage by humans [7]. Nowadays, ML techniques are used in different domains and tasks including regression, classification, speech recognition, fraud detection, and many others. Machine learning algorithms and techniques are inspired from several realms namely mathematics, neuroscience, statistics and computer science.

In general, machine learning algorithms are divided into two main steps: a training phase: the algorithm tries to learn based on the data; and a verification phase: the algorithm tests and tries to apply what is learnt.

The majority of the existing ML algorithms could be categorized in three classes: supervised, unsupervised and reinforcement learning [8]. The first class necessitates a labeled data set for the training phase in order to build a representation of the relations connecting the studied parameters. Unlike the first class, the unsupervised learning algorithms are not provided with input/output pairs. The emphasis here is mainly on classifying the data in different sets (clusters) by finding the connections between the given information. The third category, also known as the online learning, refers to process of handling the problems that an agent opposes when he must learn behavior via trial-and-error exchanges with an active environment [9].

Of course, some machine learning algorithms do not automatically fit into exactly one of these categories, there are some algorithms sharing features of both supervised and unsupervised learning approaches. The goal of these hybrid algorithms is mainly to benefit from the strengths of these two categories without inheriting their drawbacks [10].

Developing efficient algorithms that are suitable for many different application scenarios is a challenging task. Nevertheless, using reinforcement learning algorithms is the most suitable choice to solve the problem of static and non-contextual AC policies. Indeed, in our case it is sought that the algorithm must detect, progressively while accesses are made to resources and while the security policy is executing, the access control rules which are not optimal and even which present or lead to generate security problems. It is therefore an online learning.

B. Blockchain concept

Originally introduced by Satoshi Nakamoto in 2008 [11] to underpin the Bitcoin cryptocurrency network, the blockchain is a computational paradigm that consists of a distributed ledger which contains all transactions ever executed within its network, enforced with cryptography and carried out collectively by a peer-to-peer nodes. Blockchains allow us to have a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, in a cryptographically verifiable manner.

Beyond the cryptocurrency field, blockchain is spreading over several other realms: Identity management [12], reputation system [13], storing system [14], IoT [15], access control [16], etc. Moreover, the continued integration of blockchains in the IoT domain will have a considerable impact on industry, home automation, healthcare, and so on.

Blockchain is a distributed database for transaction processing. All transactions in a blockchain are stored into a single ledger. The blockchain technology is built on top of four

fundamental building blocks, each building block has key properties, and each property is achieved through specific mechanisms:

1) Identifying the source and destination of a transaction: in a blockchain based ecosystem, users serve from digital identities called "addresses" to send and receive transactions. These addresses should be self-generated (independent from any given authority) and anonymous (reveal nothing about the real identity of its owner).

2) Transactions: A transaction records the transfer of a value (altcoin) from some source address to destination addresses. Transactions are generated by the sender and broadcasted the network of peers. Transactions are invalid unless they have been recorded in the public history of transactions, the blockchain. Note that these transactions are publically verifiable, furthermore, once a transaction is recorded in the blockchain it cannot be altered without that alteration being detected and rejected by the other nodes in the network.

3) Condition for auto-processing a transaction: The transfer of any value (e.g. altcoins, tokens) with the blockchain or the execution of any function through the blockchain should be locked by a logic conditions (e.g. low, contract) that have to be written as a code and automatically executed by nodes in the network. This condition should be self-executed.

4) Consensus: Every user or node in the network relies on algorithmically enforced rules to process transactions with no human interaction required to verify in an independent way the correct execution of the protocol, and obtains the same results. Each node has exactly the same ledger as all of the other users or nodes in the network. This ensures a complete consensus from all users or nodes in the corresponding currencies blockchain.

Fig. 2 shows the process of adding a transaction to the blockchain network. It gives an overview of the logic behind this technology in a five steps.

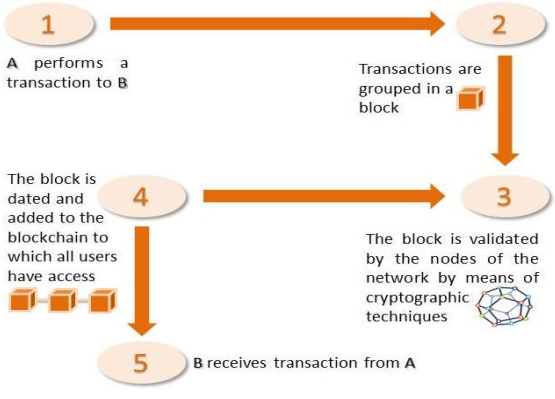

Fig. 2. Overall functioning of the blockchain concept

C. AC and blockchain

An access control model is often used to rigorously specify and reason on the access control policy.

Providing an adequate access control model for IoT services is a vital but challenging topic. Actually, authentication and authorization concepts have been treated in numerous works. However in constrained environments, there is no considerable advancement. Moreover, IoT platforms need more and more dynamic, intelligent and fully distributed access control mechanism to be compatible with its nature.

The Blockchain applied to IoT provide a new world of promise and fascinating possibilities. Actually, the decentralization, automation, and trustless features of blockchain make it an ideal candidate to become a foundational element of IoT solutions.

One integration of the blockchain technology in the IoT is presented in [17] which consider that all the IoT devices of an organization work on the same blockchain network. The organization (or the device owner) deploys a smart contract that allows them to store the hash of the latest firmware update on the network. The devices can then query the contract, find out about the new firmware, and request it by its hash via a distributed peer-to-peer file system such as IPFS. Another approach to integrate the blockchain in the IoT is presented in the framework FairAccess [4] which will be detailed in section III.

In short, blockchain or distributed ledger technologies combined with IoT as underlying infrastructure can provide the next wave of innovation that streamlines the way business operates, the same way the web did, giving birth to a new collaborative economy [18].

D. The need for a distributed AC architecture in IoT environments

The centralized approach consists in relieving smart device from the burden of handling a vast amount of access control-related information by outsourcing these functionalities to a back-end server or gateway which is responsible for security tasks. This approach presents many advantages: 1) possibility to reuse existing solutions and technologies; 2) authentication and access control policies are easier to manage in centralized IoT architectures. However, this approach presents several drawbacks: 1) prevent end to end security; 2) present single point of failure; 3) require trust foreign entities.

In distributed architecture, the access control process is carried out by the end component. This means that each device must be capable of handling authorization processes and have adequate resources to do so. In this proposal work, the concept of a distributed IoT is fundamental as a promising approach to release IoT. First of all, as devices increase their computational capacity, there are more opportunities to bring intelligence on the devices themselves. Moreover, this approach presents the following advantages: 1) end-devices act smartly, and are autonomous; 2) users have more control over the granularity of the data they produce as they are more enabled to define their own access control policies; 3) cost: it is less expensive than providing a cloud back end for each connected smart object; especially those that might need a connection for a decade; 4) trust could be supported in a better way with the decentralized approach than the centralized one because policies can be defined at the edge of the networks and there

will be no need to introduce any central entity; 5) This approach allows real time contextual information to become central to the authorization decision. However, the need to extend the constrained device with access control logic makes the implementation of this approach unfeasible in resource-constrained devices, and that is why going on with the totally distributed blockchain technology is strongly recommended.

III. Related Works

Many access control models have been proposed in the literature to address security issues in IoT. Below is a summary of the most recent and relevant ones.

A. Role Based Access Control (RBAC)

RBAC (Role-Based Access Control) [19] refers to an access control model for governing user accesses to a system's resources, based on the notion roles. This model relies on four main blocks and each one of them provides RBAC with a number of features. These blocks are the core RBAC, the hierarchical RBAC, the static separation of duty relations and the dynamic separation of duty relations. The first block is composed of five components (users, roles, permissions, operations and objects). Roles and permissions are assigned, respectively, to users and roles. Moreover, there are two separate stages in RBAC: The design phase, where the administrator of the system or the security officer can describe a number of assignments between the system's components. The second phase (the run-time phase), that consists of enforcing the assignments in the system by the model as it is specified by the security policy, which was approved throughout the first phase.

B. Attribute Based Access Control (ABAC)

In ABAC model, accesses are allowed based on the notion of attributes. In fact, these later characterize every subject and object and identify them inside the system [20]. There is two parts that compose ABAC: The policy model and the architecture model which enforce this policy. ABAC model proclaims in his standard version that access are allowed according to the subject's attributes. Moreover, it is in the policy rules that conditions under which access is granted or rejected are defined. In ABAC model, the attributes are linked with the subject and the object features. Consequently, the user is given appropriate access control permissions suitable to his attributes at the time when he sends his access request to a given object. In the literature, several works using ABAC model have treated the AC from an IoT perspective: In 2014, Ye et al. [21] have proposed an authentication and access control model for the perception layer of the Internet of Things. The designed protocol provides low storage and communication overheads to deal with the constraints in resources of the IoT context, basically in perception layer. Furthermore, the fact that the model allows accessing the data according to user attribute guarantees fine-grained access control. Though, it necessitates on the other side complex management and slows down (even block) its large deployment to constrained devices. Therefore, they only offer abstract outcomes of the proposed model.

C. Usage control (UCON)

Another famous AC model is the usage control (UCON) proposed in [22], it is considered as the next generation of access control models for the reason that it presents several novelties unavailable in traditional access control models such as RBAC and ABAC. It deals with the problems generated in the authorization phase, before the access execution, after the access execution, or even during the execution. In addition, it has the capability of supporting attribute's mutability; in other words, if a problem is produced in the security policy (during the execution) due to an alteration of some access attributes, the allowed access is canceled and the usage became invalid. Further information about UCON model is detailed in [23]. Many researches (like in [24]) have also applied UCON in collaborative system.

Before concluding this section, it is important to note that, in the state of the art level, there is a work that has stressed the particularity of UCON over usual AC models such as MAC, DAC and RBAC, and also that makes UCON more appropriate to the dynamic aspect of IoT, this work is exposed in [25].

D. Organization Based Access Control (OrBAC)

The OrBAC [26] model is one of the richest AC models in terms of components and applicability to many realistic situations; it was conceived to handle remaining issues in the extensions of RBAC. It presents an original dimension, namely the organizational concept; also it makes a clear distinction between the abstract level (roles, views, activities) and the concrete level (subject, object, action). In the decision making process, OrBAC takes into consideration various context information which can be temporal, spatial or declared by the subject (user). However, one of the big drawbacks of this model, especially when talking about IoT environments, is that it is based on a totally centralized architecture and does not provide or support the distribution, collaboration and interoperability requirements. That said, several works have done in order to extend OrBAC to overcome these limitation: PolyOrBAC [27] deals with this problem by using the OrBAC model to manage the internal policies of each organization, but to ensure the collaboration aspect between organizations, web services technology was. Nevertheless, such technologies that PolyOrBAC uses (e.g. SOA-based web services) are not systematically supported by IoT constrained nodes. To fix that, SmartOrBAC [28] and [29] objectives are to adapt OrBAC model to IoT situations. The major contribution of this proposition is the fact that it improves the notion of context (present in OrBAC) to respond to the IoT requirements. Unfortunately, SmartOrBAC does not precise any lightweight mechanisms to reduce the OrBAC complexity in order to be supported by IoT constraints devices.

The layers and components of OrBAC are shown in a simplified manner in the following Fig. 3.

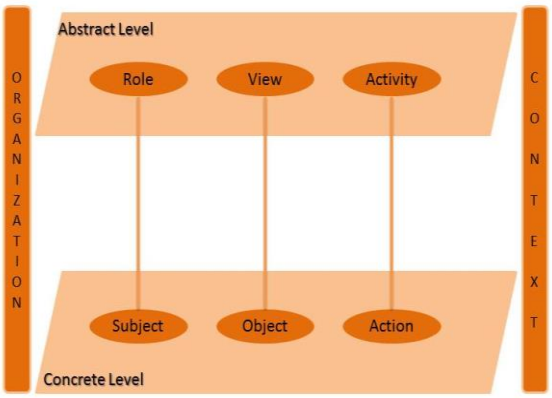

Fig. 3. Simplified presentation of OrBAC layers

IV. The Proposed Framework

In this section the focus is on the proposed framework that aims to solve the static and centralized problems of access control policy. This solution will be based on two essential concepts highlighted in the previous sections of this paper: Blockchain technology and machine learning algorithms.

A. Problem statement and research questions

Actually, most access control solutions today provide the ability for centralized authorities, whether governments, manufacturers or service providers to gain unauthorized access to and control devices by collecting and analyzing user's data. That may cause ethical and privacy problems.

Section II-D has dealt with the problems coming from the centralized architecture. However, in IoT environments, a big obstacle blocks us from adopting a distributed architecture: The constrained devices generally used in the IoT do not have the capacity of calculation nor of storage to deal with a full distributed access control process where there is no central entity responsible for managing this latter. Therefore it is necessary to make a tradeoff between the two architectures or adopt a hybrid one as in SmartOrBAC. Except that fortunately the blockchain can respond with efficiency to this problem.

Another problem encountered by access control in the context of IoT is the difficulty of managing the security policy according to the contexts especially with the colossal number of smart devices supposed to be managed in IoT situations. This leads to adopt static policies where the manager or the security officer writes all the security or access control rules in a static manner. The major disadvantage of this approach is that this policy never detects if it contains rules that lead to security problems, which create conflicts or which are not optimal. This approach never takes into consideration feedback from the results of its operation. Moreover, given the number of the increasing number of smart objects, it is almost impossible to manage this policy manually in an efficient and totally personalized way.

This new framework responds to these problems, it gives people what properly belongs to them and also present an automatically-improved and dynamic security policy.

B. IoT-OrBAC

IoT-OrBAC access model, like SmartOrBAC [28], is specially conceived for the IoT context and it is designed through an abstraction layers' perspective that makes use of a deep comprehension of the IoT paradigm as it is presented in the physical world. In the IoT that uses smart services as well as smart devices, contextual information is a key component in the decision making process, and only a real-time consideration of this information will reach smartness. In order to handle that, the authors improved the "context" concept (originally exposed in OrBAC) to fit the IoT needs. IoT-OrBAC separates the problem into several layers and then distributes processing charges between constrained devices and less constrained ones and at the same time addresses the collaborative aspect with a specific solution.

The layers IoT-OrBAC presented are shown in a simplified manner in the following Fig. 4.

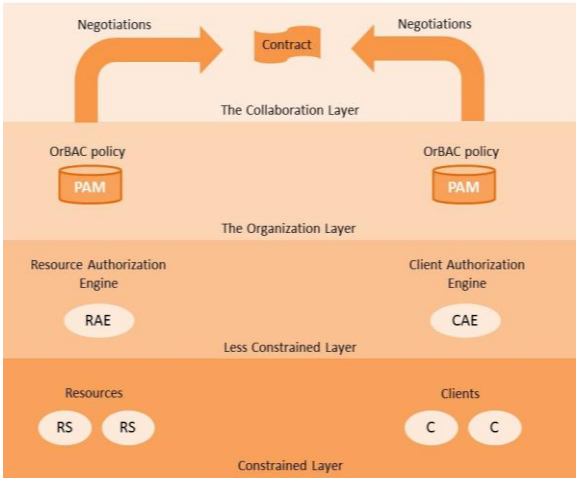

Fig. 4. Simplified presentation of IoT-OrBAC layers.

C. Fair Access

To explain how FairAccess works, let us take the following use case: Suppose that a subject (e.g., a requester device *A*, known with its address *rq*) wants to execute an action (e.g., read or alter) on a protected object (e.g., resource *B*, identified with its address *rs*). First, the subject must send this request to the authorization management point (AMP (AMP = wallet) which plays the role of a Policy Enforcement Point (PEP) that protects the requested object. The PEP formulates the received request to a *GetAcess* transaction. Then, the PEP broadcasts this transaction to the hole network of nodes with the aim of reaching miners , those later act as distributed Policy Decision Point (PDP), and accept or reject the transaction. The PDP evaluate the request and then it executes a SmartContract already deployed in the blockchain via a previous transaction called *GrantAccess*. The execution of SmartContract leads to decide whether the request should be permitted or not. Finally, if it is allowed, the SmartContract provide the requester with an access Token by sending it to his address through an *AllowAccess* transaction. After that, the Token will appear in the requester's token database.

To summarize, and as it is shown in Fig. 5, authorization process in FairAccess framework consists of: 1) registration of a new resource with a corresponding address; 2) definition of an access control policies in the form of SmartContract deployed in the blockchain by a *GrantAccess* transaction; 3) access request; 4) access allowed; 5) access revoked/updated.

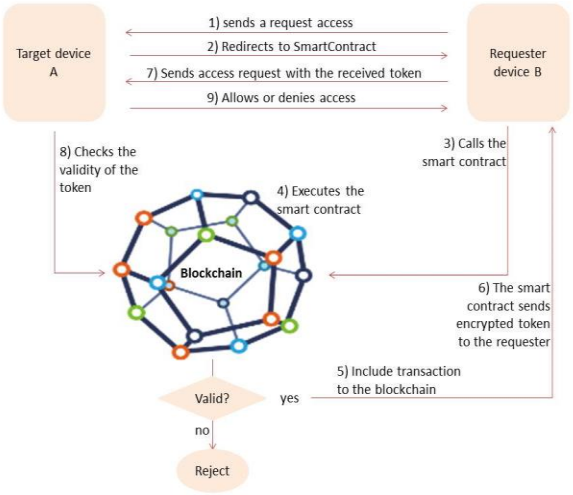

Fig. 5. Reload access control policies process in FairAccess.

D. Improve/upgrade security policy with ML algorithms

This framework uses the concept of SmartContract as a representation of an access control policy defined by a resource owner (RO), to manage access over one of his resources. It is a scripts stored on the blockchain. Since it resides on the chain, it has a unique address. This SmartContract is triggered by addressing a *RequestAccess* transaction type to it. It then executes independently and automatically in a prescribed manner on every node in the network, according to the data that was included in the triggering transaction. If the data fulfill access control policies, the *PolicyContract* will be correctly executed and then generates and assigns an Authorization Token to the sender of the *RequestAccess* transaction. For each end device, the RO defines one *PolicyContract* which is responsible for managing it access control functions.

Typically, the process of a classic reinforcement learning model begins by connecting an agent to its environment. Then, and in every interaction the agent receives some information (called feedback in this paper) about the present state of the environment; the agent then picks an action to make (output). The executed actions, obviously, updates the environment state and the value of this latter is transferred to the agent as a feedback. Note that the agent's behavior has to select actions in order to improve the situation of the environment especially in long term.

Formally, a typical RL model contains:

- A group of environment states, *S*;
- A group of agent actions, *A*; and
- A group of scalar reinforcement signals or weights if needed.

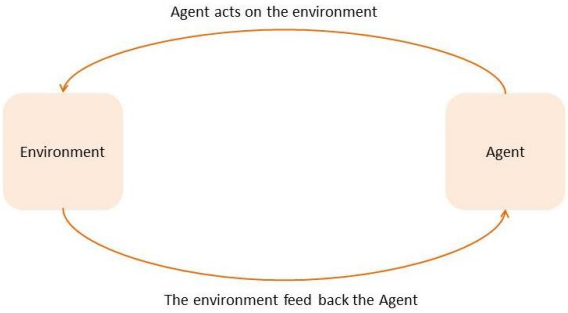

Fig. 6. Typical Reinforcement Learning (RL) scenario.

Moreover, it is important to emphasize that RL, generally, the fields of work of RL and the supervised learning (SL) are not the same (Fig. 6). Indeed, unlike SL, RL responds to problems where there is no arrangement of input/output information. Instead, the agent receives a reward (technically feedback information) after picking an action in a given state. It is indispensable that the agent passes several experiences to gather the maximum of rewards in order to know the best his environment and so he can make the right and optimal actions.

This proposed work relies on a fully distributed infrastructure based on blockchain technology as has been done in the work [4] of FairAccess. That said, it will use, as a cited before, the concept of SmartContract to distribute the security policy in the chain. Requesting access to an object will thus be managed by the detailed procedure of Fig. 5.

Once the IoT environment, now presented by the blockchain infrastructure, begins to function, it will send feedback information after each successful or unsuccessful transaction to the two entities involved in the communication, namely the subject (or requester) and the object (or resource). This information will be used as an evaluation of the transaction and its participants and will be taken into account to update the stakeholder data (e.g. update the trust, credibility or integrity levels of the participants) and also to update access control rules that allowed this transaction to be done.

E. Architecture

The procedure of this framework is detailed in the following organogram presented in Fig. 7.

Note that even if the feedback information are sent only to A and B, these information are spread to the blockchain after the update of SmartContract for example, so they become public.

Using Reinforcement Learning (RL) algorithms, the policy (the smart devices also) is trained to make particular decisions. It works this way: the SmartContract (which presents the access control policy of the smart object) is exposed to an environment where it trains itself continually using trial and error. Consequently, this SmartContract learns from past experience and tries to capture the best possible knowledge to make accurate business decisions.

The feedback information is represented by a vector with *n* number of components. These later may be binary represented (0 or 1) or with a level or weight of satisfaction (trust, integrity …) between 0 and 1.

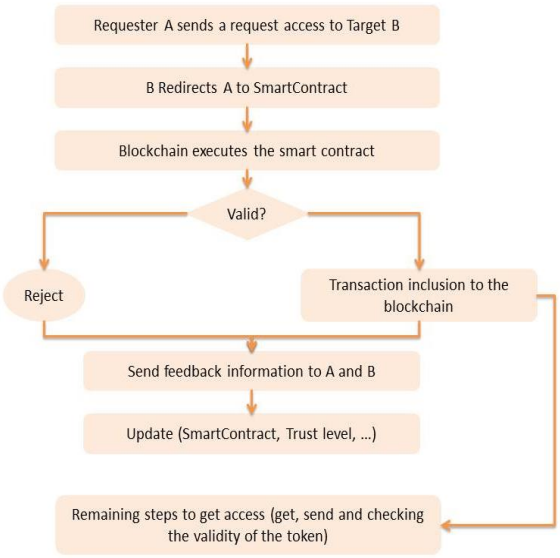

Fig. 7. Process organogram of our framework.

Let's take the very basic example: an organization H has some smart objects *(O_1, ..., O_n)*, it adds them to its security policy, it creates then and publishes their SmartContracts in the network of the blockchain. Suppose that the subjects *S_1, ..., S_m* have access to the objects *O_1, ..., O_n* based on the rules contained in the SmartContracts.

Let us suppose that after each use of an object *O_i* by the subject *S_1* (which is a legitimate user), a breakdown is noticed in the object *O_i*, the feedback of *O_i* will be zero or a low note in the credibility scale given to *S_1*. The algorithm will determine, especially if it is repeated, that *S_1* will have to be removed from authorized users, and the security policy will update.

Another case, which does not concern the credibility/trust level of users is: Let us imagine that an object *O_1* frequently encounters problems when used in a given context *C_i*. The low notes coming from several transitions under the *C_i* context lead to detect the source of the problems and thus update the SmartContract by prohibiting the use of the object *O_1* under the context *C_i*.

Note that this framework is not limited to a specific access control model, that is why the components of the feedback vector are left open, they can include the context as seen before (e.g. OrBAC, SmartOrBAC), but also The attributes (ABAC), the level of credibility (I-OrBAC [30]).

Note also the choice of a category of algorithms (Reinforcement Learning) and not a single algorithm considering that the interest here is in the online learning aspect of this category which fits with the discussed requirements. That said, each smart-object owner or organization can choose the algorithms to implement according to their needs and their objectives.

F. Algorithm & inference system

In order to present the inference system of the proposed framework, hereafter the definitions of its components:

A: The requester how wants to access the resource

B: The resource or the object

Req(A, B): Requester A sends a request access to Target B

SmartContract(B, A, S): The target B redirects the subject A to SmartContract S

GrantAccess(A, B, T): Complete the remaining steps to get access (get, send and check the validity of the token) and then Allows A to access B. Also create a transaction T.

AddBC(T): Add the transaction T to the blockchain

feed(A, B, T): send feedback information of the transaction T to A and B

update(B): Update A knowledge (SmartContract, level of credibility, trust, integrity, …)

Reject(A, B, R): Reject the request henceforth named R, deny the access of A to B

In the beginning an access request to resource B is sent by A. The output of this step is a SmartContract S. In case of failure, the result is a *Reject(A, B, R)* plus the feedback; otherwise the remaining steps to get access are executed: allowing A to access B and then generating a transaction T which can be added to the blockchain, without forgetting to send the feedback. After the feedback A's and B's knowledge are updated.

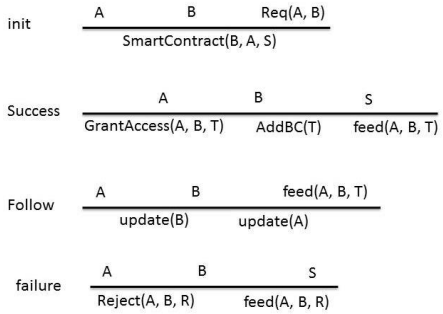

Fig. 8. Inference system of the proposed framework.

V. Conclusions And Future Works

Today, IoT is surrounding us and its aptitudes of sensing, actuation, communication, and control become ever more sophisticated and ubiquitous; however these advantageous features are also examples of security and privacy (trust among users and things [31]) threats that are already nowadays slowing down the growth and expansion of the Internet of Things when not fulfilled properly.

This work has focused on the access control in the Internet of things environments. It proposed a framework that aims to solve two problems: 1) Problems that come with the centralized architecture, without being forced to transmit the management of the access control from a central entity to the nodes of the network. Indeed, the constrained devices generally used in the IoT do not have the capacity of calculation nor of storage to deal with a full distributed access control. 2) Problems of handling the access control policies

especially with the colossal number of smart devices supposed to be managed in IoT situations. This commonly leads to adopt static policies where the manager or the security officer writes all the security or access control rules in a static manner. The new framework proposed in this paper responds to these problems, it gives people total control of their IoT devices without being forced to trust in an outside entity and also present an automatically-improved and dynamic security policy.

The proposition presented in this article is based, on one hand, on the concept of the blockchain to ensure a totally distributed infrastructure to ensure an access control without trusting external central entities. This distributed aspect is strongly recommended in the Internet of things environments as well as privacy and unlinkability. On the other, the framework relies on an "online learning" mechanism of machine learning algorithms (Reinforcement Learning) in order to provide a dynamic, optimized and self-adjusted security policy.

In this paper, we presented an introduction of the internet of things paradigm, and how the access control and security policy management are among the IoT's priorities, both at the technological and research level. We then gave more details of some fundamental notions in this work namely the concepts of blockchain, machine learning and distributed architecture. Then section III was concentrated on previous/related works done in this domain. After that a presentation of the proposed framework was given by, first, mentioning the problem statement and research questions, then by explaining the contribution of this paper to improve/upgrade security policy using machine learning algorithms. Furthermore an explication of the architecture and algorithm that operate the framework was exposed. Finally, we conclude the paper with an explicit inference system for a better understanding of this work.

However, this contribution still has some limitations on which we intend to work in our future paper. Indeed, blockchain technology presents some intrinsic drawbacks especially when talking about privacy, required time for block validation, and so on. We also pretend to complete this framework with integrating the notion of collective intelligence which will respond to privacy concerns. As a final point, this model needs also a thorough case study as well as an implementation as a concrete proof of concept.

REFERENCES

[1] J. Lopez, R. Rios, F. Bao and G. Wang, "Evolving Privacy: From Sensors to the Internet of Things", 2017, p. 1.

[2] S. Elbouanani, M. A. Elkiram, O. Achbarou, "Introduction To The Internet Of Things Security", 2015. [Accessed: 06/2017].

[3] A. Alkhalila, R. A. Ramadan, "IoT Data Provenance Implementation Challenges", *3rd International Workshop on Tasks on High Performance Computing (THPC)*, 2017, p. 3.

[4] A. Ouaddah, A. Abou Elkalam and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things", *Security and Communication Networks*, 2017, pp. 1-22.

[5] D. J. Dougherty, K. Fisler and S. Krishnamurthi, "Specifying and Reasoning About Dynamic Access-Control Policies", IJCAR 2006, pp. 632–646.

[6] T. O. Ayodele, "Introduction to Machine Learning"

[7] M. Abu Alsheikh, S. Lin and D. Niyato, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications", IEEE Communication Surveys & Tutorials, vol. 16, no. 4, 2014,

[8] Y. S. Abu-Mostafa, M. Magdon-Ismail, and H.-T. Lin, "Learning From Data", AMLBook, 2012.

[9] L. P. Kaelbling, M. L. Littman and A. W. Moore, "Reinforcement Learning: A Survey", Journal of Artificial Intelligence Research 4, 1996, pp. 237-285.

[10] O. Chapelle, B. Schlkopf, and A. Zien, Semi-Supervised Learning, vol. 2. Cambridge, MA, USA: MIT Press, 2006

[11] S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," pp. 1–9, 2008

[12] C. Fromknecht, D. Velicanu, and S. Yakoubov, "A Decentralized Public Key Infrastructure with Identity Retention" IACR Cryptol. ePrint, 2014.

[13] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," IFIP Int. Inf., 2016.

[14] S. Wilkinson, J. Lowry, and T. Boshevski, "Metadisk a blockchain-based decentralized file storage application," 2014.

[15] A. Ekblaw, A. Azaria, J. Halamka, and A. Lippman, "A Case Study for Blockchain in Healthcare:'MedRec' prototype for electronic health records and medical research data," 2016.

[16] G. Zyskind and A. S. Pentland, "Decentralizing Privacy : Using Blockchain to Protect Personal Data," 2015.

[17] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", 2016

[18] C. Scardovi, "Fin Tech Innovation and the Disruption of the Global Financial System,".

[19] R. S. Sandhu, "Role-based Access Control," Adv. Comput., vol. 46, pp. 237–286, 1998.

[20] V. C. Hu, D. Ferraiolo, R. Kuhn, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations", *NIST Special Publication*, 2014.

[21] N. Ye, Y. Zhu, R. Wang, R. Malekian, and L. Qiao-min, "An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things," Appl. Math. Inf. Sci. An Int. J., vol. 1624, no. 4, pp. 1617–1624, 2014.

[22] J. Park and R. Sandhu, "Towards usage control models: beyond traditional access control," in Proceedings of the seventh ACM symposium on Access control models and technologies - SACMAT '02, 2002, p. 57.

[23] A. Lazouski, F. Martinelli, and P. Mori, "Usage control in computer security: A survey," Comput. Sci. Rev., vol. 4, no. 2, pp. 81–99, 2010.

[24] X. Zhang, M. Nakae, M. J. Covington, and R. Sandhu, "Toward a Usage-Based Security Framework for Collaborative Computing Systems," ACM Trans. Inf. Syst. Secur., vol. 11, no. 1, pp. 1–36, Feb. 2008.

[25] G. Zhang, W. Gong, The research of access control based on UCON in the internet of things, J. Softw. (2011)

[26] A. A. E. Kalam el al., "Organization based access control," in Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks, 2003, pp. 120–131.

[27] A. Abou El Kalam, Y. Deswarte, A. Baïna, and M. Kaâniche, "PolyOrBAC: A security framework for Critical Infrastructures," Int. J. Crit. Infrastruct. Prot., vol. 2, no. 4, pp. 154–169, 2009.

[28] A. Ouaddah, I. Bouij-Pasquier, A. Abou Elkalam, and A. Ait Ouahman, "Security analysis and proposal of new access control model in the Internet of Thing," in 2015 International Conference on Electrical and Information Technologies (ICEIT), 2015, pp. 30–35.

[29] I. Bouij-Pasquier, A. A. El Kalam, A. A. Ouahman, and M. De Montfort, "A Security Framework for Internet of Things," Springer International Publishing, 2015, pp. 19–31.

[30] A. Ameziane El Hassani et al., "Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity", Int. J. Inf. Secur, Springer-Verlag Berlin Heidelberg 2014.

[31] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead", Computer Networks, 2015, pp. 146–164.