On the Application of Fuzzy Set Theory for Access Control Enforcement

Diogo Domingues Regateiro, Óscar Mortágua Pereira and Rui L. Aguiar
Instituto de Telecomunicações, DETI, Universidade de Aveiro, 3810-193, Aveiro, Portugal

Keywords: Access Control, Fuzzy Set Theory, Database and Information Security.

Abstract: Access control is a vital part of any computer system. When it comes to access to data, deterministic access control models such as RBAC are still widely used today, but they lack the flexibility needed to support some recent scenarios. These include scenarios where users and data can be dynamically added to a system, which emerged from IoT and big data contexts. Such scenarios include data from network operators, smart cities, etc. Thus, models that are able to adapt to these dynamic environments are necessary. Non-deterministic access control models fall into this approach, as they introduce new ways of mapping users to permissions and resources, but lack the auditing capabilities of deterministic models. In this paper, the usage of these models will be defended and argued for. In particular, a solution based on fuzzy set theory is proposed as it is thought to be able to provide some flexibility benefits of non-deterministic models, while giving some assurance to security experts that the resources are not accessed by unexpected users.

1 INTRODUCTION

Access control has always been an important feature on any system, be it physical or digital, as it restricts the access to a location or resource in a controlled and selective manner(Shirey, 2007). However, these types of systems are usually defined with binary permissions that either allows an entity (a human or some other system) to access that location/resource or not. The most successful access control models are usually those that mimic real world ways of managing permissions within the context of their application, of which the Role-based Access Control (RBAC)(Ferraiolo and Kuhn, 1992) model takes a central position in many of them. RBAC maps entities trying to access some resource to a role, a meaningful category within the context of the system being protected and that determines to which resources that entity may access to successfully complete their tasks. This way, RBAC can be seen as a deterministic model, since given a user its permissions are explicitly defined.

However, with the advent of the Internet of Things (IoT) and 5G, the quantity and complexity of data available that needs to be stored and processed (big data) has increased considerably. Classical storage solutions that deployed these access control models, such as relational databases, are ill-suited to handle this issue because the deterministic nature of these models require a tight mapping between users, permissions and objects(Fradique Duarte et al., 2017). Furthermore, the **real world is not always as unambiguous as these models require it to be** in their policies. For example, some documentation from European projects may not be publicly available, but access to some portions of it could be disclosed to experts researching in some area related to a project. There is no hard definition of what makes someone an expert, so normally it would have to be checked manually on a case-by-case basis. Fuzzy set theory can handle vague notions such as *expertise* or *environmental risk*, allowing it to be much more flexible with its policies while retaining the auditing capabilities due to the fact that it still is deterministic in nature. Non-deterministic models on the other hand can be much more flexible. They can use machine learning techniques or probability approaches to handle the vagueness associated with such notions and classify users on it, allowing access control decisions to be made. However, they lack auditing capabilities as permissions can change over time.

Additionally, given a big data scenario, every resource must classified manually if they are to be made publicly available or not. The application of access control when there are potentially millions of resources that are (semi-)structured and heterogeneous is then problematic, as a user request would have to be manually verified to each individual resource. Machine learning techniques can be used to classify documents based on their contents, and policies can be

Regateiro, D., Pereira, Ó. and Aguiar, R.
On the Application of Fuzzy Set Theory for Access Control Enforcement.
DOI: 10.5220/0006469305400547
In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT*, pages 540-547
ISBN: 978-989-758-259-2

written for each class the documents can be classified into. There are non-deterministic models that use machine-learning techniques to make access control decisions, which can be considered almost like a black box that takes information about the user requesting access, the document to give access to and outputs an access control decision. There are also models that make probabilistic calculations if there are missing attributes(Chen et al., 2016; McGraw, 2009) or models that calculate the risk associated with a request(McGraw, 2009).

Finally, there are those that use methods based on fuzzy set theory, classifying users in terms of fuzzy relations and fuzzy permissions over the data(Martínez-García et al., 2011). This paper will explore the usage of fuzzy set theory in more detail and contrast deterministic and non-deterministic models on their benefits and issues. Furthermore, the possibility of pairing a fuzzy model with machine learning techniques as a solution for access control in highly dynamic scenarios will be proposed as an application scenario.

This paper is divided as follows. Section 2 will provide a short background introduction into some non-deterministic access control models and techniques. Section 3 will present current state of the art related these access control models. Section 4 will present arguments in favor of such models and in particular to fuzzy sets. Section 5 will present the counter arguments to use such models. Section 6 will present solution which aims to address some of the issues found, and finally section 7 will present a brief discussion.

2 BACKGROUND

As stated, there are scenarios where the manual classification of users and data is not practical due to their dynamic nature. Systems where new users can request access at any time and/or new kinds of data, with different structure and information, can be added at runtime. It has been explained how deterministic models such as RBAC cannot handle these situations in a satisfying manner, leaving access to be defined manually from one user to some data. This section will introduce three techniques to tackle this problem: through probabilistic methods; cognitive systems; and fuzzy set theory.

Probabilistic models(Chen et al., 2016; McGraw, 2009), on the one hand, attempt to some measure of probability related to the access control decision. RAdAC attempts to take into account the profile of the user attempting to access some resource and the context of the request, such as current thread levels. From this information, a risk measurement can be calculated for a given request using probabilistic methods. A policy in this context should state the acceptable level of risk to grant access, so the calculated risk measure can be used to reach an access control decision. These models can also add additional constraints to override a high risk request, such as the operational need. Hence, if a request is allowed to be executed due to operational need, it can be granted access regardless of the risk involved.

Cognitive systems, on the other hand, are similar to a black box that takes user profiles and other inputs to provide an access control decision. This can be achieved through the usage of machine learning techniques and other methods such as reasoning, natural language processing, human-computer interaction, etc. This is the simplest method as the model only needs to be configured with the appropriate algorithms and then given a sample dataset of access control decision for training. While this allows for a request from a new user to be easily processed, it has some problems since security experts cannot easily determine what the outcome of an access control decision will be. More so if the cognitive system is allowed to learn from the access control decision it makes, allowing it to evolve over time.

Finally, fuzzy set theory involves sets where its members might only have partial membership to it. As an example, consider a liquid in a bottle labelled as 90% water. The liquid does not have a 90% chance of being water, but instead it *IS* 90% water and 10% something else. Thus, fuzzy set theory is not related to probabilistic models, as the membership values do not convey a notion of chance. It allows for more vague conditions to be used. For example, a fuzzy set could contain all the temperature values that a room feel ”hot”. A room being hot is a vague notion, but nevertheless it is possible to create a function that more or less models it. This function can take the exact temperature value, also known as the crisp value, and turn it into a membership degree to the fuzzy set just described. Hence, a temperature input of 5^{o}C could be considered to have 0% membership, at 15^{o}C it would start to rise linearly from 0% and when the input becomes 30^{o}C the membership degree is 100%. An access control model based on fuzzy set theory is still deterministic in nature, but it would be able to model vague conditions that are usually found in the real world and that are more intuitive to use by humans.

To finalize this section, all of these approaches are valid and can be used to address the problem discussed, depending on the situation at hand. Proba-

bilistic models can be used to handle unexpected situations, such as missing attributes, or situations where the access decision must take into account risk related situations. Fuzzy set theory based models allow policies to be defined based on the vague conditions that exist in the world, enabling a more natural way of expressing said policies. It also has the benefit of classifying users and data into each defined fuzzy set as they come into the system in a predictable and reliable way. Cognitive systems employ a great variety of tools, from machine learning to reasoning, to be able to generate an access control decision based on the user and the data requested, however the decision may change over time.

3 RELATED WORK

In the area of non-deterministic access control models, the techniques and approaches used to achieve non-determinism can vary significantly. (Crampton et al., 2015) argues that in cases where user attributes may be missing, the access decision may be inconclusive and a probabilistic model is used. This would lead to more than one decision generated by the access control system, a possibility also introduced by the ABAC access control model. When facing this scenario, the access control decision process can be quite complex. Instead of building an entire new evaluation mechanism based on probabilities, fuzzy set theory could assume a membership degree of 0% to the associated conditions. Depending on the conditions used and the importance of the missing attribute, the user could still be granted access.

Other non-deterministic models exist in the literature, such as DRAC (Chen et al., 2016), RAdAC(McGraw, 2009) and other frameworks(dos Santos et al., 2016). DRAC proposes a model based on risk evaluation for the cloud which uses a dynamic threshold for the risk associated with the request. The associated risk is calculated based on a sliding window of the subject's history. However, it does not differ much the ABAC model, integrating only the measured risk into the access control decision making. When it comes to handling dynamic users and data, it suffers from the same problem that deterministic models suffer. RAdAC is similar to DRAC, adding operational need to the decision making process that can override a too high risk request. In the end, it also fails to solve the issues presented in this paper.

In regard to existing deterministic models, extensions can be made to give them more functionality or make the applications built for them more secure(Pereira et al., 2014; Regateiro et al., 2014). However, the intent of applying fuzzy set theory to access control is to create a more flexible deterministic model that is not held back by previous models.

In addition, IBM(IBM, 2016) has also argued that most information regarding security is written in natural language, i.e. humans can easily understand it but machines cannot. This also means that a human cannot know every bit of information about threats and other security related information that exists. However, by using cognitive systems it is possible to analyze this type of information and include it so that, for example, new threats are accounted for when investigating some issue. This helps an analyst to have greater knowledge about the latest security threats, freeing his time to focus on other issues.

Current solutions such as IBM Watson, Microsoft Cognitive Services, Google Prediction API and Amazon Machine Learning show how important cognitive systems are becoming. However, most of these services are just APIs that allow to build cognitive services. One problem with the cognitive systems is that the algorithms used are a lot of the times opaque to the people that use them. This means that it is not possible to know what the behaviour of the system will be in every situation, specially when the system can evolve over time, which can result in the lack of trust in its correctness. Fuzzy set theory, however, follows membership functions that can be understood and visualized, allowing more easily to verify its correctness.

Finally, fuzzy set theory is an idea that has been researched in recent years to tackle use cases where authorization-related information is vague. It can be applied in two different levels(Kacprzyk et al., 2015) when it comes to its application to access to data: on the databases(Martínez-García et al., 2011; Prade, 1984; Buckles and Petry, 1982; Ma, 2006) or on the querying language(Bosc and Pivert, 1995; Bosc and Pivert, 1992b; Bosc and Pivert, 1992a).

In (Martínez-García et al., 2011) the authors present an access control model based on RBAC that is applied on the database level. The model uses fuzzy sets to model the relations between subjects, roles and the permissions. Such a model can handle some uncertainty when it comes to the degree a subject actually plays a certain role and what permissions are actually granted. However, this model is restricted to using the role associated with each user and does not handle other attributes directly into the access control process.

An example of the application of fuzzy set theory on the querying language level is SQLf(Bosc and Pivert, 1995), an extension made from the SQL language, where vague querying is achieved on regu-

lar databases. Instead of applying fixed predicates in queries, such as querying accounts with balances over some particular number, they can be created that use fuzzy conditions in the predicates. For example, given a table with account balances, it would allow to query for entries where the account balance is *high*. This allows for more intuitive queries to be written when exactness is not needed for the results returned. However, this approach also does not solve the issue mentioned in this paper, as it only applies to the querying procedure and not the decision-making.

4 GROUNDS FOR FUZZY ACCESS CONTROL MODELS

One of the arguments used to justify the inclusion of fuzzy access control models in computer systems is the fact that the real world is not always unambiguous by nature, specially when it comes to human interaction. This includes human decisions which can be influenced by many external factors such as human language which can convey the same information in a multitude of ways and is oftentimes vague and dependent on context, emotions, etc.

Access to resources can also be seen as another form of human interaction. Person A possesses data that other people want to access, and so person A sets conditions that must be met for access to be granted in their policies. When humans enforce the access control policies, it is possible to process the subjectivity inherent in some of the access requests. However, when it comes to computer systems, it is not generally the case due to their unambiguous nature.

Non-deterministic models allows computer systems to capture the subjectivity and vagueness of the human world. These can include the conditions that do not have a concrete definition but that are used by humans constantly in speech, such as the example of someone *being an expert* in some area, through training. While deterministic, fuzzy set theory is particularly good in capturing these vague notions but taking inputs that can be used to define them - in the case of *being an expert* it would mean values like number of publications, number of citations, etc - and use a function to map those inputs into a membership degree. In this sense, a person does not have to either be an expert or not at all. Instead, someone can be partially an expert, like 40%, working their way higher but still not considered to be like a person who does not know anything of said area.

In fact, a policy based on fuzzy set theory can grant access to someone provided they have some minimum degree of membership to a fuzzy set. To reiterate, fuzzy sets are defined by a domain of elements and a function that takes values from that domain and maps them to a membership degree between 0 and 1. Furthermore, fuzzy logic uses a generalization of two-valued logic to support values any between 0 and 1, meaning that vague conditions can be used together in logical expressions. Since the logic used is a generalization, a condition that is precise is allowed in such a model, with membership functions that either output a membership degree of 0 or 1 for a given input. Thus, it becomes simple to categorize users based on their attributes and policy defined fuzzy sets automatically. These fuzzy sets can represent the users that can access a certain resource, with a different fuzzy set for each permission if required. A defuzzification process can then be carried out to map the membership degrees to access control decisions.

Fuzzy-based models also have the benefit of being easier to audit and analyze when compared to cognitive based solutions. Fuzzy set theory is based on membership functions to sets, which are well defined. On the other hand, cognitive systems use a collection of technologies and methods to learn from information and to be able to perform reasoning over it. For example, a cognitive system, given enough information about access attempts and the corresponding access decision, is able to categorize access requests and answer with a decision. However, auditing such a system is hard, as the model used to reach a decision is based on training data, complex machine learning techniques and reasoning. As such, a cognitive system is many times considered to be a black box in a system that takes certain inputs and outputs an answer.

Fuzzy set theory is also beneficial for IoT and big data contexts where a big amount of data is generated and/or new data-sources can dynamically appear. A model based on fuzzy set theory can categorize resources based on several attributes, such as its origin, contents, and other (meta-)information. The classes that a given classifier classifies resources into can be defined in the policy. Alternatively, resources can be classified beforehand. These classes can then be associated with the fuzzy sets that denote permissions within that class, to which a subject must have some degree of membership to be granted the associated permissions.

Regarding probabilistic models, they usually output more than one access decision, depending on the probability values. In the case of the model presented in (Crampton et al., 2015), missing attributes are modelled as a non-deterministic attribute retrieval process. The process is extended to be a probabilistic attribute retrieval and probabilistic tools are used for imple-

mentation. While these can possibly be used to implement a model with similar goals as a fuzzy set theory based model, it does not exactly support vagueness in the same way. For example, using a probabilistic model, a subject can have some chance of being an expert, but in the end it means that it either is, or it is not an expert. Fuzzy set theory allows for users to be partial experts, a notion that is closer to reality.

To summarize, when it comes to scenarios where the conditions for granting access to data are vague or there is a high dynamism of users and resources, such as in IoT and big data scenarios, non-deterministic access control models pose an interesting solution. However, models based on fuzzy set theory are able to handle a large number of new users without the need for manual permission granting. Furthermore, resources that are added to the system can be categorized into security classes that, based on the membership degree of a user to one or more fuzzy sets, can allow those resources to be made available instantly. Finally, fuzzy set theory allows security experts to audit the correctness of the access control system more easily when compared to other solutions such as cognitive systems, since membership functions are deterministic and can be analyzed.

5 CHALLENGES AND ISSUES

There are several claims that can be made against non-deterministic and fuzzy access control models being used in computer systems. These range from model specific issues to the ethics surrounding the fact that computer systems are being allowed to grant or deny access to a resource without human intervention.

The first issue that can be raised with the usage of non-deterministic access control models is detailed in (Matzner, 2016), where the notion of a gap between the perceived situation between a human and a cognitive system differs. This difference is branded as ”the model gap”. The model gap itself is not a problem, but instead it is the main feature of a cognitive system. Deploying human operators to analyze the output of a cognitive system is often thought to be enough to address the ethical problems related with the automation. Hence, it is important to reflect on this model gap when deploying a non-deterministic model, in which the presentation and description of the system are necessary so ethically problematic judgments do not occur by recognizing the difficulty of independent judgment.

Note that this issue is not confined to non-deterministic models, but since deterministic models follow a set of static rules imposed by a human, the issue is not as great and problems can be resolved rather easily by a human operator by adding another rule. Non-deterministic models require an easy way for a human to control it and grant or deny access to a user. RAdAC(McGraw, 2009) achieves this by taking into account the notion of ”operational need” with a request. If the operational need is allowed by the policy, then it can override the risk measurement. Models based on fuzzy set theory can, for example, do something similar, such as using a fail-safe fuzzy set that acts like a regular set. Members of this set are granted membership by a human operator and it grants the user the associated permission. Another solution is to add explicit rules just to handle these situations. Cognitive systems require a human operator to keep teaching it whether an access control decision is correct or not, so that wrong access decisions get corrected.

Auditing can also play a part in the issues these models face. By becoming more complex, using techniques ranging from algorithms to artificial intelligence to arrive at access control decisions, it becomes harder for the policies of these models to be verified that they behave exactly as intended. Risk-based models can change their access control decision outputs based on the risk levels and cognitive systems can be setup to learn over time. Fuzzy set based models can have their membership functions mathematically checked to determine the inputs where the decision is *grant* or *deny*. However, the formulas involved can depend on various input variables, so the analysis may be quite complex as well.

Another fair concern is misconfiguration of the models themselves. While deterministic models tend to be very straightforward in what conditions can a user access some resource or not, the non-deterministic are not. Risk measurements procedures and training datasets all need to be considered for the access control policies creation. In more complex scenarios that involve many variables to grant access to a resource, slight misjudgments may go unnoticed. This is why it is important to have a close monitoring of the decisions such a security system makes so these misconfigurations of the policies can be detected. While fuzzy models are deterministic, the membership functions also need to be carefully designed to represent the vague notions associated with them.

As mentioned, models based on fuzzy set theory require membership functions, which are used to define the fuzzy sets by mapping a membership degree of an element to the set. These membership functions, in an access control system, can take attributes of the users as inputs to map them into various fuzzy

sets, which can represent roles, relations, or something else. Where risk-based models can use thresholds to make the access control decisions (even if the risk measurement can be quite complex) and cognitive systems automatically create the needed inner configuration from the training set, models based on fuzzy set theory do not. Membership functions need to be defined manually or using some machine learning method like cognitive systems. While fuzzy set theory is great at capturing vagueness and vagueness, it requires some work to create the policies, even if the membership functions are not usually too complex and are usually simple truncated triangles in shape.

Since models based on fuzzy set theory require membership functions, it is important that the attributes a user has can be validated as they are used to map the users to fuzzy sets. This can be a problem, since to be sure that the attributes a user has are correct and have not been modified, an Identity Provider (IdP) must exist that can validate and sign them. In the case of the access to the European project documentation, trusted Universities could be accepted at IdPs for their users, as well as citation databases and other similar entities so that the expertness of a user can be determined. So, a use case where these kind of access control model is deployed must consider the IdP to use for the users.

Finally, computer resource concerns can also be raised. While models that function by using and following a set of access control rules are usually fast and not very heavy computationally, cognitive systems require a big base of information to perform adequately, and since they have to process said information base they can be quite computationally intensive as well. Nevertheless, models based on fuzzy set theory can be less computationally intensive than cognitive systems, since they do not require a large training dataset to operate. To summarize, when using these models it is important to keep in mind the ethical issues since machines and humans perceive contexts differently. Furthermore, the potential for a model policy to be verified as being correct should be considered, as well as the model configuration complexity and how computationally intensive it can become.

6 PROPOSED SOLUTION

A solution, consisting of a possible model and architecture, will be proposed here that aims to handle the use cases mentioned thus far. The idea will be for the system running this solution to take in large amounts of data while allowing new users to be able to access them based on vague linguistic notions. Fuzzy set theory is able to define these notions while retaining its vagueness by allowing users to be partially matched to them.

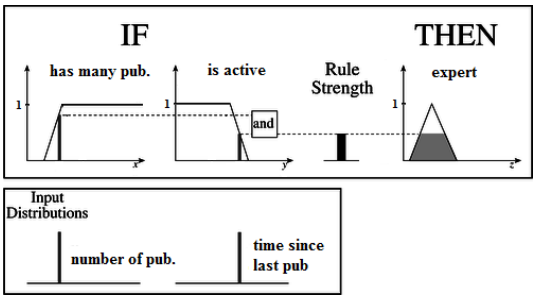

Figure 1: Partial fuzzy inference system diagram example.

6.1 Model

Figure 1 provides a simple diagram of how such a system could work. The lower section indicates the input distributions used by the system, which are the user attributes. These distributions are mapped by the membership functions into fuzzy sets that model vague notions, matching a user partially or fully to them via a membership degree. Then, the membership degree for each notion is used to calculate a rule strength. This rule strength can then be used to qualify the user in terms of an output notion, such as how much of an expert the user is. Several of these output notions can be used, each derived in the same manner, to arrive at an access control decision.

In the European project documentation example provided, a user has two attributes, which could be signed by an University IdP: **number of publications** and **time since last publication**. These are discreet values, shown as vertical bars on the real number line.

Then, the system would recognize that the resource that is being requested has some security label (not shown in the figure) that requires the user to be an expert in an area to be able to access it. A security label is placed on a resource to indicate which characteristics the user must possess to be granted a permission, such as reading access. For this example system, a user is recognized as being an expert if they have many publications **AND** are active researchers in the area. This would be defined in the policy as a rule using the fuzzy controller language, for example.

Number of publications and **time since last publication** are vague notions. For the system to handle these, each is mapped to a fuzzy set. In the Figure 1 it is possible to see the membership functions associated with them in the *IF* section, and how the **number of publications** and **time since last publication** of the user are not enough to grant him total membership. In fact, it is possible to say that the user is close

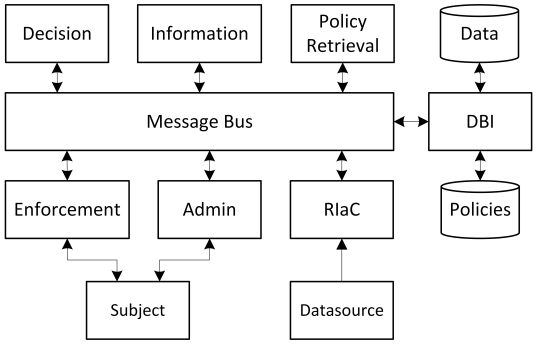

Figure 2: Fuzzy set based model architecture.

to having many publications according to this policy, around 80%, but is only around 50% active. Nevertheless, the policy still recognizes the user as being partially an expert - around 50% - given the provided rule strength, which was calculated by applying the *AND* operator on both membership degrees, which takes the smallest of the two.

What is left is to arrive at the access control decision. This is a simple case where only one rule is used, but note how there is a function under "expert". This function is known as an output membership function and it is truncated at the rule strength. From it, a value $z*$ from the z domain is chosen as an output value using a process known as defuzzification. There are many methods to achieve this depending on the use case, but as an initial approach, a threshold z_t value could be used. Then, $z*$ could be obtained by selecting the smallest z value that maximizes the truncated function. If $z* < z_t$, then the user is denied the permission, else the user would have it granted. If more than one rule is used, such as the user having to be an expert and not young, then the function obtained from the union or the intersection of the output membership functions of each rule is used.

6.2 Architecture

A possible architecture to implement this model is shown in Figure 2. This architecture is based on the XACML architecture, mostly due to its modular approach, and encompasses several modules and other components. This is only one architecture amongst many that could be used. The various modules that are proposed in this architecture are:

- **Subject:** A human or service that uses the system.
- **Datasource:** A source of resources to be protected by the system.
- **Enforcement:** The module that enforces access control decisions.
- **Administration:** The module that handles administration requests, such as the creation and alteration of policies.
- **RIaC:** The Resource Ingestion and Classification module. It handles the resources sent by datasources and classifies them to associate security labels so the system knows which fuzzy sets to apply to them when access is requested.
- **Decision:** The module that runs the fuzzy inference system to arrive at an access control decision.
- **Information:** Handles information requests made by the decision module in its operation, be it from the defined policies, user attributes or some other environmental attributes.
- **Policy Retrieval:** Retrieves policies as needed by other modules.
- **DBI:** The DataBase Interface module to access the datastores. Handles requests for data and policies.
- **Message Bus:** A tool used to interconnect all modules of the system.

A subject, when they need access to some resource in some way, sends a request to the enforcement module through some public API along with an identifier, such as a token. The enforcement module will then dispatch the request to the decision module for evaluation. The decision module then requests the access conditions and associated fuzzy sets to match the user attributes to the information module, which will request the required policy to the policy retrieval module if needed. Finally, the policy retrieval module may request the policy from the policy datastore to the DBI module.

Once the required information propagates back to the decision module, membership degrees of the user to the various fuzzy sets are calculated and a final access decision is made as detailed in section 6.1. The decision is then sent back to the enforcement module that enforces the decision made. Administration related requests are made to the Administration module instead, which can have an authentication layer. Multiple instances of each module can be used as well, allowing the architecture to scale as needed.

Finally, testing such a model and architecture for correctness can be more challenging since to allow large amounts of data to be ingested by the system, it needs to classify each document automatically using some method. However, assuming that the documents are well classified, the correctness of the system can be assured by analyzing the membership functions and how the $z*$ value depends on the input values provided.

7 DISCUSSION

In this position paper, a position to use non-traditional access control models, and in particular fuzzy set theory, was defended and argued for. What makes fuzzy set theory so interesting is its capability to handle vagueness and conditions that are vaguely worded.

These types of models were found to have several issues, which included the ethical questions of computer systems and humans perceiving a context in different ways, their more complex inner workings which makes auditing the correctness of the policies harder and the difficulty of creating the policies themselves. However, these models are capable of handling scenarios with a big amount of users and resources automatically, being an interesting choice for IoT and big data scenarios. Furthermore, situations where access conditions are ambiguous or there are many variables to consider can also be handled.

A solution, comprised of an idea for a model based on fuzzy set theory and an architecture, was also proposed which aimed to be able to take advantage of the points raised in this paper while trying to address some of the issues that were found as well. This solution will be studied further, especially in terms of correctness validation, and a working proof of concept is expected to be implemented in the near future.

ACKNOWLEDGEMENTS

This work is funded by National Funds through FCT - Fundação para a Ciência e a Tecnologia under the project UID/EEA/50008/2013 and SFRH/BD/109911/2015.

REFERENCES

Bosc, P. and Pivert, O. (1992a). Fuzzy logic for the management of uncertainty. chapter Fuzzy Querying in Conventional Databases, pages 645–671. NY, USA.

Bosc, P. and Pivert, O. (1992b). Some approaches for relational databases flexible querying. *Journal of Intelligent Information Systems*, 1(3-4):323–354.

Bosc, P. and Pivert, O. (1995). SQLf: a relational database language for fuzzy querying. *IEEE Transactions on Fuzzy Systems*, 3(1):1–17.

Buckles, B. P. and Petry, F. E. (1982). A fuzzy representation of data for relational databases. *Fuzzy Sets and Systems*, 7(3):213–226.

Chen, A., Xing, H., She, K., and Duan, G. (2016). A Dynamic Risk-Based Access Control Model for Cloud Computing. In *2016 IEEE Int. Conf.s on Big Data and Cloud Comp., Social Comp. and Networking, Sustainable Comp.*, number 2014, pages 579–584.

Crampton, J., Morisset, C., and Zannone, N. (2015). On Missing Attributes in Access Control. In *Proc. of the 20th ACM Symposium on Access Control Models and Technologies*, pages 99–109, NY, USA.

dos Santos, D. R., Marinho, R., Schmitt, G. R., Westphall, C. M., and Westphall, C. B. (2016). A framework and risk assessment approaches for risk-based access control in the cloud. *Journal of Network and Computer Applications*, 74:86–97.

Ferraiolo, D. and Kuhn, D. (1992). Role-based access controls. *15th National Computer Security Conf.*, pages 554–563.

Fradique Duarte, F., Domingues Regateiro, D., Mortágua Pereira, Ó., and Aguiar, R. L. (2017). On the Prospect of using Cognitive Systems to Enforce Data Access Control. In *Proc. of the 2nd Int. Conf. on Internet of Things, Big Data and Security*, pages 412–418.

IBM (2016). Cognitive Security White Paper. Technical report.

Kacprzyk, J., Zadrożny, S., and De Tré, G. (2015). Fuzziness in database management systems: Half a century of developments and future prospects. *Fuzzy Sets and Systems*, 281:300–307.

Ma, Z. (2006). *Fuzzy Database Modeling of Imprecise and Uncertain Engineering Information (Studies in Fuzziness and Soft Computing)*. Secaucus, NJ, USA.

Martínez-García, C., Navarro-Arribas, G., and Borrell, J. (2011). Fuzzy Role-Based Access Control. *Information Processing Letters*, 111(10):483–487.

Matzner, T. (2016). The model gap: cognitive systems in security applications and their ethical implications. *AI & SOCIETY*, 31(1):95–102.

McGraw, R. (2009). Risk-Adaptable Access Control (RAdAC). *in:Privilege (Access) Management Workshop. NIST–National Institute of Standards and Technology–Information Technology Laboratory*.

Pereira, Ó. M., Regateiro, D. D., and Aguiar, R. L. (2014). Extending RBAC Model to Control Sequences of CRUD Expressions. *Intl. Conf. on Software Engineering and Knowledge Engineering*, (January):463–469.

Prade, H. (1984). Generalizing database relational algebra for the treatment of incomplete or uncertain information and vague queries. *Information Sciences*, 34(2):115–143.

Regateiro, D. D., Pereira, Ó. M., and Aguiar, R. L. (2014). Distributed And Typed Role-Based Access Control Mechanisms Driven By CRUD Expressions. *Int. Journal of Computer Science: Theory and Application*, 2(1):1–11.

Shirey, R. (2007). Internet Security Glossary, Version 2. Technical Report 9.