On the Prospect of using Cognitive Systems to Enforce Data Access Control

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

Keywords: Cognitive Systems, Access Control, Information Security, Nondeterministic Models, CogDAC.

Abstract: Data access control is a field that has been a subject of a lot of research for many years, which has resulted in many models being designed. Many of these models are deterministic in nature, following set rules to allow or deny access to a given user. These are sufficient in fairly static environments, but they fall short in dynamic and collaborative settings where permission needs may change or user attributes may be missing. Risk-based and probabilistic models were designed to mitigate some of these issues. These take a user profile to determine the risk associated with a particular transaction or fill in any missing attributes. However, they need to be maintained as new security threats emerge. It is argued in this paper that cognitive systems, as part of a more general Cognitive Driven Access Control approach, can close this gap by learning security threats on their own and enhancing the security of data in these environments. The benefits and considerations to be made when deploying cognitive systems are also discussed.

1 INTRODUCTION

Most data access control models in widespread use today have addressed data security using a deterministic only approach. From these, the Role Based Access Control (RBAC) model (Sandhu et al., 2000) is probably the most well-known and most widely used. In fact, most, if not all Relational Database Management Systems (RDBMS) (e.g. Microsoft SQL Server, Oracle, PostgreSQL, etc.), as well as most of the web development frameworks in use today (e.g. ASP.NET, Spring, etc.) support some form of its implementation.

The deterministic nature of these models, however, presents some limitations to their expressive power (Pereira et al., 2014)(Crampton et al., 2015). One such limitation has to do with the fact that the access decision can only be computed if all the input values of authentication are presented. Another limitation stems from the fact that these models are based on static access rules and so authentication parameters are not expected to be highly variable.

Given the above limitations, deterministic models are therefore not well suited for highly dynamic scenarios, such as those becoming prevalent in the IT landscape with the emergence of new computing paradigms and technologies, of which Big Data, NoSQL, the Internet of things (IoT) and Cloud Computing are some examples.

On the other side of the spectrum non-deterministic approaches have been proposed to deal with some of these shortcomings. These models further extend the deterministic ones by incorporating non-deterministic techniques into the access decision computation (Crampton et al., 2015)(Cheng et al., 2007). These characteristics mean that these models are more flexible and have greater expressive power then their deterministic counterparts. A consequence of this greater flexibility however is the increased complexity of their implementation.

The Risk-Adaptable Access Control (RAdAC) model (McGraw, 2009) is an example of a non-deterministic model and is also part of a new paradigm of access control based on risk. RAdAC provides support to risk by incorporating operational need and security risk into the access decision. The contribution of each of these factors in the computation of the access decision will in turn vary according to the situational conditions of the access request. Because of this, RAdAC allows a greater flexibility in the range of policies it supports, from the more restrictive ones to the more relaxed ones, in

Duarte, F., Regateiro, D., Pereira, Ó. and Aguiar, R.
On the Prospect of using Cognitive Systems to Enforce Data Access Control.
DOI: 10.5220/0006370504120418
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 412-418
ISBN: 978-989-758-245-5
Copyright © 2017 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

which operational need may override the security risk if such risk is considered to be acceptable by the policy. To be successful however this model needs processes capable of computing several different metrics associated with user trustworthiness, IT component protection capabilities and the threat level associated with their hosting environment as well as past access decisions. Furthermore, adequate policies must be formulated and properly translated to a machine understandable format. Carrying out such task in a manual or semi-automated manner can prove to be unfeasible or too complex and expensive in terms of time and resources.

Cognitive systems may offer a solution to this problem. These systems are expected to learn and reason in a continuous fashion through the ingestion of huge amounts of data and by interacting with their human operators. These systems are also devised to understand natural language in textual and spoken form and seem therefore ideal to automate most of the processes discussed above. A cognitive system may also present the advantage of aggregating all these processes into a single unified system.

IBM Watson (High, 2012), the cognitive system developed by IBM to participate in Jeopardy in 2011 is probably the most well-known example of such a system. Since then, many other IT giants have invested in this area and are already offering their own cognitive products. Microsoft and Google are such examples. This is a thriving arena and the range of the field of application of cognitive systems is increasing rapidly. IBM for example has already proposed the application of Watson in several fields and as diverse as life sciences research, healthcare and cyber security.

Given such a context, it can therefore prove to be of great interest to discuss the feasibility, appropriateness and the possible implications and limitations of the inclusion of cognitive systems as active pieces on the data access control process. The intent of this paper is therefore to serve as a contribution to such a discussion. The conceptual implementation of a cognitive system is however not addressed. It should also be noted, that the use of cognitive systems, to address access control related challenges in this case, can be further generalized as an example of the use of cognition. This generalization can be thought of as a Cognitive Driven Access Control (CogDAC) approach to access control.

The remainder of this paper is structured as follows: Section 2 introduces cognitive computing and cognitive systems. Section 3 presents the state of the art in data access control. The arguments and counter arguments concerning the usage of cognitive systems as data access control mechanisms are discussed in Sections 4 and 5 respectively. Finally, Section 6 presents an application scenario for cognitive systems in access control and Section 7 presents the conclusions and concludes the paper.

2 BACKGROUND

Cognitive computing is a technological approach whose main purpose is to allow for a more natural interaction and collaboration between humans and machines (Zikopoulos et al., 2015). This collaboration is paramount in scenarios of ever increasing complexity, such as those posed by Big Data, where the sheer volume and speed at which information is generated far surpasses the human ability to process it (Y. Chen et al., 2016).

This new concept of system is generally referred to as a cognitive system and greatly differs from the traditional programmable computing systems. Cognitive systems learn how to perform a task as opposed to be programmed on how to perform it and keep learning and improving themselves thru continuous data ingestion and interaction with their human operators (Zikopoulos et al., 2015). These systems are often characterized by three fundamental principles: learn, model and generate hypotheses (Hurwitz et al., 2015).

Cognitive systems learn continuously. This learning process leverages huge amounts of data, commonly referred to as the corpus, which represents the knowledge base of the system. This data generally encompasses a specific domain of knowledge. Ultimately the cognitive system should be capable of disambiguating conflicting information and properly choose the appropriate sources of data relevant to its own knowledge base, by itself and with minimal human intervention.

Cognitive systems also generate models. That is, upon the ingestion of data, concerning a specific domain of knowledge, the system generates an internal model. This model is the machine understandable representation of that domain and is continuously refined to improve the system's performance and accuracy. The quality of the data ingested by the system and its completeness concerning the domain of knowledge to be captured, greatly influence the quality of the model which in turn impacts the overall system's performance.

Finally, when questioned by a human operator, the system should generate not just a single response, but several candidate hypotheses instead. Evidence

supporting each of the generated hypotheses should be gathered to score and rank them and ultimately decide on the most suitable candidates to be presented to the human operator along with all the supporting evidence used in the process. This allows for the human operator to be able to take a better and more informed decision by being given proper insight on how the different responses were computed.

3 STATE OF THE ART

Traditional access control mechanisms are based on deterministic decisions, i.e. given a user with one or more attributes only one decision can be made. However, it may happen that a user does not possess one or more attributes required for a decision to be made as explained in (Crampton et al., 2015). This paper argues that in those cases the access decision may be inconclusive and more than one decision generated by the access control system, a possibility also introduced by the Attribute Based Access Control (ABAC) model. This shows how complex the access decision making procedure can be when not all information is present, making deterministic models not always the best solution. However, instead of building an entire new evaluation mechanism based on probabilities, it is argued here that a cognitive solution could be implemented to deal with the problem presented. Furthermore, it could attempt to arrive at more intuitive decisions than a simple probabilistic model could achieve.

Other nondeterministic models have been proposed in the literature, such as the Dynamic Risk-Based Access Control (DRAC) model (A. Chen et al., 2016), the already mentioned RAdAC (McGraw, 2009) and other frameworks (dos Santos et al., 2016). DRAC proposes a risk-based model for the cloud, which uses a dynamic threshold for the risk associated with each access. This risk is calculated based on a sliding window of the subject's access history. However, it still follows set rules based on ABAC, integrating only the risk assessment into the decision making. Furthermore, a misconfiguration of the policies or a badly adjusted risk assessment system may not lead to a more secure system. In the case of RAdAC, a cognitive system could be used to assess the risk associated with a request by using information from the user, the environment and the request itself.

In (Chen Gu et al., 2009) the authors argue that current access network technologies lack the ability to "self-perceive, self-configure, self-learn, and self-heal" intelligently. They further state that cognitive is the approach to take these challenges on and that it is the reason it has been a hotspot for research in the recent years. This position adheres in part with ours, in which cognitive solutions can be used in access control scenarios where self-awareness of security threats can be an important factor.

The usage of fuzzy logic to implement access control mechanisms is an idea that has been researched in recent years to tackle use cases where authorization-related information is vague. In (Martínez-García et al., 2011) the authors present one such access control model based on RBAC. The model uses fuzzy relations between subjects and roles and between roles and permissions. Such a model can handle some uncertainty when it comes to the degree a subject plays a certain role and what permissions are allowed for them. However, this model lacks in context awareness to accept additional parameters other than roles.

In (Zheng et al., 2016) the authors state that due to the limited and unreliable nature of human memory, relying on it to store and retrieve secrets, such as passwords, is one of the main problems when it comes to network security. To address this issue, it is proposed that cognitive techniques could be used to authenticate users or devices based on pattern recognition of behaviors or the correlation of information obtained from various devices. Then, traditional authentication techniques can be supported by these techniques to provide a higher assurance that the authentication is legitimate. However, the proposed architectures are meant for authentication only, and therefore fail to bring the full capabilities of cognitive systems into the access control procedure on other levels such as decision enforcement.

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 or her 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 and not a full-fledged solution which this paper aims to support.

4 ARGUMENT

The traditional way of modeling the real-world access control policies uses models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), RBAC, etc. These ease the policy validation process, since the deterministic outcomes give assurances that the system will work as expected when given the expected input. However, they also lack the context awareness to adapt to new situations when unexpected inputs are given, something that a cognitive system could manage and learn from by applying reasoning and Machine Learning techniques.

When security policies take on complex scenarios that involve huge amounts of data available to be accessed (Big Data), it is not easy to perform permission auditing to be certain that the protection achieved is adequate once deployed and is visible to malicious users. For example, unknown exploits or inadequate access rules that allows users to deduce information they should not be able to know are not considered in most models, since these are statically enforced. Hence, security breaches that originate from inadequate access rules to a database are hard to detect. If a cognitive system is used instead, non-legitimate access attempts could be detected faster and reported to a human supervisor by reasoning what information the user has accessed and what can be inferred from it. Furthermore, the cognitive system can be taught existing patterns to known attacks and other new security related information that are disclosed on reliable sources.

Another point to be made is that the very act of enhancing security rules to address some vulnerability that was found. This very act is knowledge that is usually not used by any system when enforcing the access control policies. The type of vulnerability and how it was found and exploited could reveal further problems that could help protect the data if treated and processed by a cognitive system. This way, a cognitive system does not have to replace the human portion out of the security auditing process. Instead, it aids them to find issues and make access decisions based on multiple attributes and other information such as the access history and attack patterns.

So far it has been stated here that cognitive systems can be used to detect patters in, and learn from, security breaches by pooling from the vast amount of information available (books, papers, internet blogs, etc.) to categorize and help with the process. However, there are other avenues in which cognitive systems may be used. Consider a use case where a lot of information is being stored continuously on some document database and there is interest in making some portion of it available to the public, with or without some restrictions. Without a very specific structure, the data being stored cannot be easily categorized. A cognitive system can be used to process the information and categorize it so the appropriate security labels are associated with it and the information made available faster.

Another aspect regarding the use of cognitive systems is that they can analyze a user's profile, find patterns and make decisions based on it. For example, it could determine some user to be of high risk to allow access or to restrict their permissions based on some of their attributes. A cognitive system could analyze a user's online public information, such as the last places they visited and recent interests, to determine if they can be allowed to access the data requested.

Regarding deployment in enterprise scenarios, as cognitive systems evolve, more and more solutions will start to emerge to offer these benefits. Such is the case with IBM, which is working to provide a cognitive system to detect and analyze security breaches and other types of vulnerabilities with a cognitive monitoring system, and Amazon, Microsoft and Google with their Machine Learning and cognitive APIs. As the number of APIs and vendors increase, the potential for better and more mature cognitive systems also increases, and it is believed that the future of access control will be very heavily influenced by them.

Finally, cognitive systems are not only applicable to access control to databases, but also when it is enforced by a human to access some physical resource. A human operator can make mistakes in judgement or be bribed. While a cognitive system can also arrive at wrong access control decisions, it can be taught from these events systematically and process more information than any human operator could ever be capable of processing. However, having a computer system make decisions for a human can be seen as ethically problematic (Matzner, 2016). Regardless, 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.

To conclude, cognitive systems are a useful tool not only to process data and information that might otherwise be lost, but it can also enhance a human operator ability to enforce security access decisions by factoring many other attributes about the subject requesting access. When applied to databases, a cognitive system can determine if a subject should be given access to a resource by learning from a dataset of previous access attempts. Furthermore, a cognitive system can factor in many subject, resource and environmental related information to detect changes

in subject behavior and other threats that could pass unnoticed to a simple rule-based system.

5 COUNTER ARGUMENT

Traditionally, the implementation of access control systems is based on three concepts: access control policies, models and mechanisms (Samarati and de Vimercati, 2001). In this context both the security properties of the system as well as its theoretical limitations can be proved and properly bounded respectively by the formal representation of the policies, that is, the model. In the case of a cognitive system this assessment may be more difficult to achieve as it may prove challenging to provide a formal model that can accurately express non-determinism in a formal way.

The access control mechanism itself is typically characterized by at least four properties: tamper-proof, non-bypassable, security-kernel and small (Samarati and de Vimercati, 2001). From these, the first and the last two can pose some concerns when addressing cognitive systems.

Concerning the first property, tamper-proof, it should be stated that a cognitive system, as opposed to traditional programmable systems, is in an ongoing change. That is, the system should continuously learn to improve itself. In the worst-case scenario, the system can tamper itself due to this continuous changing process. The corpus, that is, the knowledge base of the cognitive system also poses concerns in this regard, as the data ingested directly reflects its behavior. Untrusted sources of information can potentially alter the system in subtle ways, by continuously feeding it malicious data over time. This type of attack can be very hard to discern or even prevent.

The last two properties, security-kernel and small, deserve also some remarks. Cognitive systems are far more demanding in terms of infrastructure and are certainly larger and more complex when compared with traditional deterministic systems such as the ones that implement DAC, MAC, RBAC, etc. Cognitive systems need to ingest and process large amounts of data in a timely fashion to allow for the decision making. On top of this the system must generate, score, rank and provide evidence in a potentially high number of hypotheses to compute every access control decision, increasing the time to reach a decision. This decision in turn must consider context and, for the machine to perceive context, techniques and algorithms such as Machine Learning, Artificial Neural Networks and Natural Language Processing must be used. Thus, for a cognitive system to be of any use, the underlying software and hardware architectures must allow for parallelism and distributed data management. This also means that the cognitive system can potentially be composed of many small components spread over many different parts of the system, making it hard to discern its boundaries. Such a system can be harder to assess and verify.

Another factor to take into account is the so called "before the fact audit" (Ferraiolo et al., 2016), one of the prominent features of RBAC and also a desired feature of access control. What this means is that it is possible to audit the permissions of users as well as the access rules assigned to the resources of the system. In a cognitive system, such a review may not be easy to perform. Concerning the review of the permissions of the user, as these are determined in terms of probabilistic models they are therefore volatile. Reviewing the access rules assigned to the system resources can also prove difficult, as policies must be translated into a suitable form, often mathematical, becoming more opaque to human interpretation. In this regard the cognitive system can be seen almost the same as a black box.

In terms of its implementation and deployment in the enterprise, the adoption of a cognitive system can also prove to be costly and challenging. Also, some expertise on the subject is required to properly train, configure and continuously assess for the proper behavior of the cognitive system over time and as policies change within the enterprise. This in turn may lead to a scenario of vendor lock-in or high vendor dependency.

Finally, there might be ethical or even legal compliance concerns, posing some doubts about the implementation of a cognitive system as an access control mechanism. This can be of particular importance in highly sensitive scenarios, where the access to data is legislated and noncompliance may implicate legal sanctions, such as the HIPAA legal framework (Congress, 1996). Leaving the access decision entirely to the cognitive system in this case can raise traceability and accountability problems in case of improper disclosure of data or non-conformity. Ultimately cognitive systems as a technology are still not mature enough as opposed to other deterministic access control models such as RBAC. Furthermore, the probabilistic nature and black box approach of such systems can prove difficult for their adoption in highly sensitive scenarios.

Table 1 summarizes the information discussed thus far between the techniques used in deterministic and non-deterministic models, which is based on our experience and the literature. The scale follows a low (L), medium (M), high (H) metric. The categories for comparison are as follows: ease of configuration

Table 1: Techniques comparison table.

	Deter.	Non-Deterministic		
	Rules	**Fuzzy**	**Probability**	**Cognitive**
EoC	H	M	M	L|M
EoPV	H	M	M	L
EoPA	H	M	L	L
DepC	L	M	M|H	H
PDet	L	L	M	H
ContA	L|M	M	M|H	H
TfD	L	M	M|H	H
AMP	L	M	H	H
NPI	L	L|M	M|H	H
EthI	L	M	M|H	H

(EoC); ease of policy validation (EoPV); ease of permission auditing (EoPA); deployment cost (DepC) in terms of computational power and storage; pattern detection capability (PDet); context awareness to take additional parameters into consideration (ContA); time for decision (TfD), i.e. the time required to reach a decision after a request is made; acceptance of missing parameters (AMP) when a request is made; impact of a new policy on configuration (NPI) in terms of reconfiguration and time required to enable it; and the amount of ethical issues (EthI).

To conclude, cognitive systems bring great promise to address the new opportunities instilled from Big Data and the growing complexity derived from a more interconnected world, but also new challenges to the access control research field.

6 APPLICATION SCENARIO

This section presents a use case for cognitive systems taking as an example a generic scenario where the RAdAC model is to be deployed. In this scenario, cognitive systems can be used as a solution to the many challenges associated with the deployment of this model, particularly: user information, IT component information, access control policy and determining security risk.

Concerning the assessment of the user's trustworthiness, it is expected that many sources of information may be used (e.g. personal information or background, authored papers, etc.). Natural language processing can ingest all this information in whatever formats it may present itself (e.g. written, spoken, video, etc.) and generate a model of the user. In this regard, the cognitive system may even present more advantages in cases were more information is needed, by actively searching for that information. Moreover, existing user models can evolve with each interaction with the user. As a final advantage, by possessing models of the users of the system, the cognitive system can actively search for indications of misuse patterns and act accordingly.

Similar reasoning applies to the task of determining the security robustness and threat levels associated with IT components and their hosting environments. In this case the cognitive system can actively monitor trusted online sources to obtain updated information about security attacks and vulnerabilities, as well as reports on certification and auditing of several IT systems with whom it may have had interactions in the past. The cognitive system can then leverage all this information to generate models of these IT systems. An added benefit is that in this way the enterprise can more easily adhere to industry security standards while keeping its system up to date security-wise.

Finally, a cognitive system can further prove useful concerning the creation of the access control policy. By leveraging its capability to understand natural language, the cognitive system could be given examples of policies used in the past to solve similar security needs. From these, new policies could be derived according to the needs at hand or assist human operators in such tasks. The cognitive system could even help in finding and solving possible ambiguities, conflicts and inconsistencies in the policies. A direct consequence of this is that by involving a cognitive system in the whole process, the policy can be stated in both human and machine understandable formats at the same time.

Given its capability to perceive context, such as environmental and situational factors, its ability to learn from past decisions and integrate that knowledge into future decisions to improve itself, the cognitive system can then compute the security risk and make an access decision.

In terms of implementation, each of the processes mentioned above could be implemented in its own cognitive system, or alternatively integrated into a single one. In the case of multiple cognitive systems, the access decision could then be derived by some sort of voting quorum system and executed in parallel to achieve better performance.

7 CONCLUSIONS

In this paper, the usage of cognitive systems in access control decisions has been argued, mentioning its many benefits, shortcomings and other issues, which are summarized on Table 1. When it comes to cognitive systems deployment in security settings, it is held back especially due to the lack of ease of configuration, policy validation, permission auditing, higher deployment costs and ethical issues.

However, cognitive systems can bring higher flexibility in terms of detecting hidden patterns – or lack thereof – in access attempts, as well as processing a large amount of authentication attributes even in complex scenarios.

Finally, an application scenario for cognitive systems in risk-based access control (RAdAC) has been presented, which aims to demonstrate some of the many contributions that one can expect to obtain from the application of such a solution.

It is undoubtful that cognitive systems are going to be central and seeing a lot of research surrounding them in the future, considering that the amount of data and information available that needs to be processed is increasing and that not all of it is structured. It is our intention to keep following and researching this topic closely, as it shows potential for new technologies and features.

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

Chen, A. et al., 2016. A Dynamic Risk-Based Access Control Model for Cloud Computing. In *2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom)*. IEEE, pp. 579–584.

Chen, Y., Argentinis, E. and Weber, G., 2016. IBM Watson: How Cognitive Computing Can Be Applied to Big Data Challenges in Life Sciences Research. *Clinical Therapeutics*, 38(4), pp.688–701.

Chen Gu et al., 2009. Cognitive access control in cognitive heterogeneous networks. In *2009 IEEE International Conference on Communications Technology and Applications*. IEEE, pp. 707–711.

Cheng, P. et al., 2007. Fuzzy Multi – Level Security : An Experiment on Quantified Risk – Adaptive Access Control. In *2007 IEEE Symposium on Security and Privacy(SP'07)*. pp. 222–227.

Congress, 104th United States, 1996. Health Insurance Portability and Accountability Act of 1996.

Crampton, J., Morisset, C. and Zannone, N., 2015. On Missing Attributes in Access Control. In *Proceedings of the 20th ACM Symposium on Access Control Models and Technologies - SACMAT '15*. New York, New York, USA: ACM Press, pp. 99–109.

Ferraiolo, D.F. et al., 2016. A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications. *NIST Special Publication 800-178*.

High, R., 2012. The Era of Cognitive Systems: An Inside Look at IBM Watson and How it Works. *International Business Machines Corporation*, 1(1), pp.1–14.

Hurwitz, J.S., Kaufman, M. and Bowles, A., 2015. *Cognitive Computing and Big Data Analytics*, John Wiley and Sons, Inc.

IBM, 2016. Cognitive Security White Paper. Available at: http://cognitivesecuritywhitepaper.mybluemix.net/ [Accessed January 11, 2017].

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

Matzner, T., 2016. The model gap: cognitive systems in security applications and their ethical implications. *AI and SOCIETY*, 31(1), pp.95–102. Available at: http://dx.doi.org/10.1007/s00146-013-0525-4.

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

Pereira, O.M., Regateiro, D.D. and Aguiar, R.L., 2014. Extending RBAC model to control sequences of CRUD expressions. In *Proceedings of the International Conference on Software Engineering and Knowledge Engineering, SEKE*. pp. 463–469.

Samarati, P. and de Vimercati, S.C., 2001. Access Control: Policies, Models, and Mechanisms. In *Foundations of Security Analysis and Design*. pp. 137–196.

Sandhu, R., Ferraiolo, D. and Kuhn, R., 2000. Standard, The NIST Model for Role-Based Access Control: Towards a Unified. In *Proceedings of the Fifth ACM Workshop on Role-Based Access Control*. pp. 47–63.

dos Santos, D.R. et al., 2016. A framework and risk assessment approaches for risk-based access control in the cloud. *Journal of Network and Computer Applications*, 74, pp.86–97.

Zheng, Y. et al., 2016. Cognitive security: securing the burgeoning landscape of mobile networks. *IEEE Network*, 30(4), pp.66–71.

Zikopoulos, P. et al., 2015. *Big Data Beyond the Hype A Guide to Conversations for Today's Data Center*, Mc Graw Hill Education.