Issues and Challenges of Access Control in the Cloud

Francesca Lonetti and Eda Marchetti
ISTI-CNR, Via G. Moruzzi 1, Pisa, Italy

Keywords: Access Control, Cloud, Testing.

Abstract: Cloud computing offers scalable and efficient information sharing and storage resources. However, the risk of security breaches for personal and private data in this computing environment is very high. Access control is among the most adopted means to assure that sensible information or resources are correctly accessed. This paper provides an overview of main access control models in cloud infrastructures discussing most important challenges. In particular, focusing on access control policy specification, analysis, verification and enforcement, we also identify some emerging issues and point out some solutions and future research directions for cloud computing.

1 INTRODUCTION

Nowadasys, the management of (personal) data becomes extremely important in many distributed environments, especially when it involves data that are subject to different regulations depending on the context in which they are stored or accessed.

In particular, the General Data Protection Regulation [1] only allows the processing of such data on the basis of specific measures or safeguards rules that may vary depending on the European or Member State laws.

Thus, mechanisms for accessing of personal data should guarantee the sufficient level of protection: i.e. the processing is not legitimate without the consent of the data subject, which must be expressed beforehand through specific access control policies. Unfortunately, in the recent modern multi-cloud environment, possibly distributed all over the world, problems may also emerge with respect to the dynamic transmission and adaptation of (personal) data when access control policies deal with data belonging to different countries, which provide different degrees of data protection, or different local realities, which may have own data format or specific data restrictions.

Just as real world common example: consider the situation in which a seafarer EU citizen is frequently moving around ports in different countries. In the unlucky case in which he/she may have health problems, there could be serious difficulties in obtaining the best medical treatment, because doctors visiting him/her could not have the access to the patient's medical history or ongoing treatments. This problem is currently mitigated by the enforcement of the General Data Protection Regulation, because it will set a uniform legislation across all EU Member States, but will still imply significant issues when transferring data to non-EU countries. Access control adaptation and interaction are just some of the multiple factors preventing continuous data storing and sharing in cloud computing environments. However, conventional access control models suffer from the lack of flexibility and scalability in attribute management and are not able to cope with the heterogeneity and variety of cloud services.

In this paper, we provide an overview of the well-known access control models, such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC), Attribute Based Access Control (ABAC) (Ubale Swapnaja et al., 2014), highlighting their limitations in cloud computing. Then, we present some specific access control proposals for cloud environments and review the most important issues and challenges concerning the distributed access of data through the multi-cloud infrastructures.

Testing and verification of access control policies are key aspects to enhance the security level of cloud environments. Traditional testing and analysis systems have to face many issues and challenges preventing their adoption in cloud environments. In this

[1] EUR-Lex Access to European Union law: http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046

Lonetti, F. and Marchetti, E.
Issues and Challenges of Access Control in the Cloud.
DOI: 10.5220/0006948702610268
In *Proceedings of the 14th International Conference on Web Information Systems and Technologies (WEBIST 2018)*, pages 261-268
ISBN: 978-989-758-324-7

specific context, we discuss in more detail the issues and challenging concerning the policy specification, analysis, testing and enforcement of XACML-based access control systems, trying to provide some possible solutions and future research directions.

The rest of this paper is structured as follows. Section 2 briefly introduces the main access control models. Section 3 overviews the main issues and challenges for access control systems in the cloud infrastructures. Section 4 focuses on possible solutions and future research directions in the context of XACML-based access control policies specification, refinement, analysis, testing and enforcement whereas Section 5 draws conclusions.

2 CURRENT RESEARCH ON ACCESS CONTROL IN THE CLOUD

Cloud computing models greatly improve the efficiency of information sharing providing scalable storage resources. Traditional access control models that authorize the access to shared data have to face new challenges to support cloud based applications. We briefly describe below the main conventional access control models and their limitations in cloud computing (Ausanka-Crues, 2001; Youniand Kifayat and Merabti, 2014):

- Mandatory Access Control (MAC) model (Ubale Swapnaja et al., 2014): a central authority is in charge of giving access decisions to a subject that requests access to a resource. This model is very expensive and difficult to deploy in cloud computing since it does not support separation of duties, delegation or inheritance aspects.
- Discretionary Access Control (DAC) model (Ubale Swapnaja et al., 2014): this model grants the owners of objects the ability to control access to their objects, according to the identities of users or their membership. DAC model is generally less secure than mandatory access control model, so it is used in environments that do not require a high level of protection The DAC cannot be used in cloud computing since there is no mechanism or method to facilitate the management of improper rights (e.g. risk awareness), which owners of objects can give to users.
- Role Based Access Control (RBAC) model (Ubale Swapnaja et al., 2014): it is the most used in organizations and enterprises. The idea is to assign rights according to the role or membership that a subject can have. Defining the right roles that represent a system and dividing subjects into categories based upon roles is not an easy task in cloud computing.
- Attribute Based Access Control (ABAC) model: it relies on a set of attributes of subjects, resources and actions in order to allow or deny the access to the resources. Security policies specify the attributes that have to be considered for making a decision. However, selecting what kind of attributes should be used, and how many attributes are considered for making access decisions is a complex task in cloud computing (Jin et al., 2012). XACML (eXtensible Access Control Markup Language) is a standard language that implements attribute-based access control (OASIS, 2005). It is a platform-independent XML-based language for the specification of access control policies. Briefly, an XACML policy has a tree structure whose main elements are: PolicySet, Policy, Rule, Target and Condition. The PolicySet includes one or more policies. A Policy contains a Target and one or more rules. The Target specifies a set of constraints on attributes of a given request. The Rule specifies a Target and a Condition containing one or more boolean functions. If the Condition is evaluated to true, then the Rule's Effect (a value of Permit or Deny) is returned, otherwise a NotApplicable decision is formulated (Indeterminate is returned in case of errors). The PolicyCombiningAlgorithm and the RuleCombiningAlgorithm define how to combine the results from multiple policies and rules respectively in order to derive a single access result.
- Risk-Based Access Control (RBAC) model: this model uses different kinds of risk levels associated with environmental conditions for giving access decisions (Suhendra, 2011). However, this model is difficult to be deployed in cloud computing because of the amount of analysis required and number of systems to be merged to compute risk levels.
- Usage based access control (UCON) model (Park and Sandhu, 2002; Bertolino et al., 2014b): The UCON model is an extension of the traditional access control models that, besides authorizations, introduces new factors in the decision process, namely obligations, conditions, and mutable attributes. It deals with new requirements for access control brought by the distributed environment. The main idea is that attributes related to subjects and objects could change their values, while the access is in progress in such a way that the access right does not hold anymore. Then, the

model allows to interrupt the access to preserve the system security. For this reason, UCON policies specify whether a decision factor must be evaluated before and/or during the usage of the resource (continuous policy enforcement).

We refer to (Cai et al., 2018) for a more detailed description of these access control models and a performance comparison among them.

Many proposals address access control problem in cloud computing leveraging and enhancing existing models (Youniand Kifayat and Merabti, 2014).

The paper in (Youniand Kifayat and Merabti, 2014) proposes an access control model able to ensure the secure sharing of resources among potential untrusted tenants, and to support different access permission to the same cloud user giving to the user the ability to use multiple services securely.

Task-Role-Based Access Control scheme is another access control approach which has been proposed for health care systems in the cloud computing environment (). Permissions in this model are activated or deactivated according to the current task or process state. This scheme was implemented in the Amazon Elastic Compute Cloud (Amazon EC2).

Tsai and Shao (Tsai and Shao, 2011) propose a reference ontology framework using Role-Based Access Control model allowing multiple roles for a subject in different sessions as well as role hierarchy based on domain ontology and transferred between various ontology domains. This model has to ensure granting access decisions in a reasonable time and according to system requirements and is scalable with respect to the number of roles, number of permissions, size of role hierarchy, and limits on tenant-role assignments.

Another ontological model for access control policies is presented in (Veloudis et al., 2016). It enhances the attribute based access control scheme by capturing a wide range of relevant contextual attributes, and enabling the policy-related knowledge to be extended and instantiated to suit the needs of any particular cloud application, independently of the code employed by that application. These contextual attributes can be associated at the level of the access control policy, indicating the contextual conditions that must be satisfied by an entity in order for an access request to be permitted (or denied)as well as at the level of the request itself, indicating the actual context attached to an entity at the time of the request (Veloudis et al., 2017).

A recent proposal presents an Access Control Model for Cloud Computing (AC3) (Youniand Kifayat and Merabti, 2014) that is compliant with the cloud access control requirements. This model is able to support different access permissions to the same cloud user for the different services. The proposed model takes into account the role and task principles, and classifies users according to their actual jobs. Dynamic and random behaviours of users are controlled by a risk engine that credits consumers according to their access behaviours.

3 ISSUES AND CHALLENGES

Considering the problem of accessing distributed (personal) data, collected though multi-cloud infrastructures, the following main challenges could be highlighted:

1. `Continuous access`: the distributed data need to be accessible from the owners independently by the organization or the country where the data are collected. The data owners must be able to continuously access the data, or delegate the access rights to a third party in case of specific conditions/problems. Technically, different users should be able to specify policy rules and those are not affected by when resources or subjects change their temporal, spacial or status conditions.
2. `Different regulations`: Different countries in which the access control entities are located may have different regulations for accessing data. This can cause security threats (Sharma et al., 2017).
3. `Dynamic access policies`: Conventional access control models in cloud computing would miss of flexibility in attribute management and scalability in dealing with a large number of users, different classification, high dynamic performance, mobility features and changes in high frequency (Wang et al., 2011). Recently, the security community has recognized the importance of dynamicity in security. Indeed, the distributed management of (personal) data sharing should be ruled by innovative, flexible, accessible, dynamically modifiable, and legally compliant access control policies, which may let the specification of precise rules and environmental conditions under which an entity/person can access to own data.
4. `User-friendly management`: The specification of access control policies is very important. Users (administration, citizen, customers, etc.) should be able to easily express (and possibly modify) them at different level of detail avoiding the risk of errors and without affecting the cloud service provisioning, code deploying and general management. The development of on-line user-centric,

user-friendly, adaptable and compliant solutions (dashboard, APIs, interface) able to perform verification and testing activity should be integrated into the Cloud context (Bertolino et al., 2014a).

5. `Continuous control`: Cloud computing can be very complex and sophisticated due to the dynamic nature of the clouds resources. Access to (personal) data cannot be granted once and for all. Multi-cloud application framework must be developed enabling secure and resilient cross-border continuous control of data access so to promptly take in place possible predictive and corrective actions. Instead of waiting for the harmful consequences, predictive security mechanisms and strategies must be developed or integrated to testing and verifying possible policy conflicts and mitigate the risk and flaws of data access configuration (Calabrò et al., 2018). Multi-cloud application frameworks should therefore allow scalable, context-aware, secure and resilient access control systems, able to monitor, control and testing the data sharing among several entities, through different channels, and by exploiting heterogeneous means.
6. `Scalability`: Cloud-based access control systems have to deal with a large number of cloud users having different access permissions. These users must be able to use multiple services according to authentication and login time (Wang et al., 2011; Almutairi et al., 2012).
7. `Resource sharing and interoperability`: To allow resources sharing among untrusted users, access control models deployed in the cloud have to support transfer of customer' credentials across layers to access services and resources (Almutairi et al., 2012). Heterogeneity and variety of services as well as diversity of access control policies and various access control interfaces can cause interoperability issues (Tianyi et al., 2011).
8. `Validation and verification of access control policies`: As access control policies can be complex and error-prone, it is very important to validate the implemented policies (specified for instance in the standard XACML notation) against the intended rights, which can be formally defined (by a model) or informally expressed, e.g. in tabular form (Bertolino et al., 2016). Moreover, also solutions aiming to verify the access control rules against some defined access control properties have to be put in place (Hwang et al., 2010).
9. `On line tracing of access control polices execution` Continuous tracing of policy execution allows to detect inconsistencies in the policy specification and provides support for policies updates if new events occur. Moreover, it can help to predict security threats due to policy modifications or combinations. It gives the ability to verify correct policy deployment and activation compliance (Lonetti and Marchetti, 2018).
10. `Testing of access control systems` Access control testing is crucial in cloud based access control models, since testing facilities enhance the level of security needed in such environments. Policy and rule combining algorithms are defined in many access control languages. Testing the right behavior of these algorithms is important when different policies and rules are combined in cloud environments and assures that there are no leaked privileges because of the syntactic or semantic errors (Bertolino et al., 2014c).

4 POLICIES SPECIFICATION, REFINEMENT, ANALYSIS, TESTING, AND ENFORCEMENT

In this section, we provide more details about possible issues, challenges and solutions useful for defining access control infrastructures able to specify, analyse, and test networking policies addressing the data management in the cloud environment. In particular, in the following subsections we target the policy specification, refinement, analysis, testing, and enforcement in the case of XACML-based access control systems.

4.1 Policy Specification

Concerning the policy specification, currently different solution for policies specification and analysis are available such as (Weimer and Vining, 2017). These proposals usually rely on the large variety of policy languages available in literature, which mainly follow three different specification approaches:

- rule-based, as for instance XACML (OASIS, 2005) and FACPL (Margheri et al., 2017), where policies are basically used to express Event, Condition, and Action (ECA) rules. The target is to enable or improve the cross-platform interoperability and modelling security aspects;

- logic-based, as e.g. ASL and PDL (Ma et al., 2015) which let to express authorization policies based on user's identity credentials and authorization privileges, to propagate the access rights among roles and groups of users, and to define integrity checks on authorization decisions;
- ontology based,as e.g. KAoS and Rei (Ma et al., 2015) which permit to represent the contextual information of an access control system (i.e., the knowledge of the system) or Veloudis at al. (Veloudis et al., 2017) that provide an ontological template for expressing the relevant contextual attributes associated to an access control policy or request.

Even if there are proficient fields of research targeting policy specification, domain IT skilled experts are still required for correctly and extensively define the required rules (policies). The current state of the art could be improved by the introduction of expressive, flexible, and user-friendly policy specification languages defined by a simple, yet rich, syntax and a rigorous semantics, amenable for verification and validation. In particular, due to the widespread diffusion of access policy usage, existing proposals, should be enriched by features supporting also the policy specification from non IT expert. This should requires the implementation of automated and reliable applications to map the user-friendly (natural language) rules into processable and machine readable policies.

4.2 Policy Refinement, Monitoring, and Testing

Once policies are specified in high-level language, they need to be automatically transformed into policies in the languages of the various enforcement points and then fine-tuned to the operational constraints of the devices where those are enforced. The action refinement theory (Rensink and Gorrieri, 2001), is typically used in formal methods for converting the specification of an (abstract) action into a (concrete) process. In the context of security, some proposals like (Martinelli and Matteucci, 2011) address this theory and provide a mechanism for transforming high-level primitives/actions into lower level processes, in such a way that some security properties are preserved within the transformation. After the policy refinement, due to the complexity of languages used from the various enforcement points for specifying the access policies and to the growing size of these policies, testing that the enforced policies properly implement the intended regulations becomes a compelling and challenging task (Bertolino et al., 2016).

In this field, a critical issue is the generation of an efficient test suite. Many methodologies and tools for the automated test cases generation from an XACML policy have been developed (Bertolino et al., 2013). Existing test cases generation tools rely on combinatorial approaches of policy values and have been proven to be effective in the automated generation of access requests (Hu et al., 2011).

Another important challenge, in the context of cloud-based access control policy testing, is to guarantee the compliance between the security requirements the policy authors intend to specify and those that the policies actually state. Moreover, combinations and integration of policies coming from different cloud based organizations increase the risk of inconsistencies. A main research direction envisages the specification of access control policies by means of a model and the usage of model-driven approaches for the generation and testing of the automatically derived security policies (Bertolino et al., 2014a). These approaches have the main goal of overcoming the difficulties of directly writing XACML code and allow the testing of XACML policies against the intentions expressed in the model.

In such a context innovative testing approaches able to discover inconsistencies between the processable policy specification and the true intentions of the users in granting/denying accesses are still necessary. In particular solutions should focus on:

- providing innovative testing strategies aiming at verifying the constraints, permissions and prohibitions defined in the processable policy;
- providing tool support for fault tracking and discovering so to promptly identify the errors in the processable policy causing inconsistencies, problems and/or security risks;
- providing facilities for verifying the correct and compliant integration of access policies coming from different areas (for instance: hospitals, legal context, generic environment and or organization constraints) with the aim of warning the user whether the final processable policy specification could allow access rights not reflecting the user original intentions;
- providing supports for checking the compliance of the processable policy with data protection and access data regulations.

4.3 Policy Analysis

The increasing spread of policy-based specifications has prompted the development of multiple analysis

techniques like, e.g., property checking and behavioural characterisations. Such techniques have been implemented by means of different formalisms, varying from multi-terminal binary decision diagrams (MTBDD) to different kinds of logics. Current proposals include (Arkoudas et al., 2014): change-impact analysis of XACML policies to study the consequences of policies modifications; logic-based analysis to verify structural properties of XACML policies: policy redundancy to increase the evaluation performance of access control systems.

However, available semantic-based approaches should be leveraged so to better analyze the properties and the structure of policies. The use of these properties will increase the confidence on the grained or forbidden system behaviours and could represent a bases for more complex analyses, as e.g. change impact analysis and redundancy minimisation. Furthermore, specific approaches enabling effective and efficient automated verification of these properties so to provide a concrete support to the security and structural analysis should be also provided. For instance, there is the necessity of specific formalisms that, on one hand, permit to collapse hierarchical policies into a single-layered representation and, on the other, are sufficiently flexible to deal with multiple domain values for attribute assignments.

In this activity, main challenges are the hierarchical structure of policies, the presence of conflict resolution strategies, the intricacies deriving from the many involved controls and the difficulties in checking whether a given security property is properly enforced.

Moreover, it is also necessary to improve and extend the list of relevant properties, concerning the three main security principles of confidentiality, integrity, and availability, and devise a general approach for rendering them in terms of policy-based specifications. To this purpose, formal methods and techniques for defining the semantics of policy languages in rigorous ways could be adopted and modified in order to provide a precise formalization of the conditions under which a policy properly enforces the intended properties.

4.4 Policy Enforcement

Many works address policy enforcement aiming to provide authorization framework and conflict resolution approaches. Usually, the available solutions involve strategy for policy precedences, cryptographic solutions or combining algorithm for solving conflict at run-time.

Runtime testing and monitoring of the policy enforcement enable to detect inconsistencies, or security flaws in the implementation of the access right enforcements (Bertolino et al., 2014a). Indeed, a runtime testing framework should: let the combination of different testing strategies; provide coverage and performance measures; let simulations on the policy evaluation engine; provide a continuous control during the runtime execution. To this purpose, in order to make easier the control of policy enforcement, a possibility is represented by the use of obligations (Margheri et al., 2017), i.e. additional actions specified in the policies that must be successfully executed at enforcing time.

However, automatic framework equipped with continuous authentication and authorization mechanisms are still necessary. In particular, research should be focused on development of strategies and tools for:

- analyze the weaknesses of the today's popular access rights languages, such as XACML and SAML, when applied to highly dynamic environments;
- provide effective and efficient extensions of such languages so to be adapted to satisfy the cloud environmental requirements;
- analyze whether today's identity management mechanisms are sufficiently mature to meet the privacy-specific requirements;
- investigate dynamic policy management infrastructure that will allow on-the-fly update of authorization policies according to the user localization;
- put in place enforcement mechanisms of authorization policies taking into account the legal aspects;
- improve existing solutions so to be easily adapted to different specific domains;
- allow possible conflicts resolution of multiple policies written in different policy languages as well as different policy instances written in the same policy language.

4.5 Mapping Issues and Challenges

Considering the issues and challenges identified in Section 3, we provide in Table 1 the solutions for policies specification, refinement, analysis, testing, and enforcement, listed in the previous subsections, that are currently addressing these challenges. The target is to highlight how the current state-of-the practice for defining access control infrastructures is replying

Table 1: Policy Specification, Refinement, Testing, Monitoring, Analysis and Enforcement *vs* Cloud Challenges.

	Specification	Refinement	Testing	Monitoring	Analysis	Enforcement
Continuous access				✓		✓
Different regulations		✓				
Dynamic access policies				✓	✓	
User-friendly management	✓					
Continuous control		✓	✓	✓	✓	
Scalability						✓
Resource sharing and interoperability			✓	✓		
Validation and verification of access control policies	✓		✓			
On line tracing of access control policies execution				✓		
Testing of access control systems			✓	✓		

to the several critical peculiarities of the cloud-based environment.

As in the table, monitor and testing are currently the most adopted solutions for replying to the listed challenges. Specifically, the possibility of on-line logging and tracing of access control systems seems to be the most effective way for behavioral control so to avoid security flaws and assure interoperability.

Moreover, still according to the table, most of the proposals are focused on the continuous control evidencing its peculiarity and specificity in the complex and heterogeneous cloud computing environment.

Finally, the table suggests also that research activity should be more focused on the possibility to integrate different regulations, to provide a user-friendly management, to improve scalability and to promote validation and verification of access control policies, because only few proposals are currently available.

5 CONCLUSIONS

Cloud computing infrastructures provide a cost effective mechanism to share hardware and software resources in a scalable and distributed way. Security is a primary concern in modern cloud interconnected distributed systems and access control represents an important security aspect specifying which subjects can access which resources under which conditions.

In this paper, an analysis of the traditional access control models as well as of new existing solutions for access control in the cloud has been provided. Then, many important challenges related to the distributed data access in cloud systems, such as continuous control, different access regulations, scalability, dynamic access policies, user friendly management of access control policies, have been discussed.

Specifically, testing and analysis of access control systems has been considered as a key feature to enhance the security level of data in the cloud. Current state of the practice solutions for policies specification, refinement, analysis, testing and enforcement have been depicted and mapped on the identified access control challenges. Possible improvements as well as future research directions have been also highlighted.

It is out of the scope of this paper to provide an exhaustive survey of issues and challenges of access control in the cloud. However, besides the existing proposals, the research activity concerning the access control in the cloud is not keeping the pace with the quick, dynamic and continuous cloud evolution. There is still the need of innovative and advanced solutions targeting the many evolving issues evidenced in this paper.

As future work, we plan to have an in-depth investigation of the research directions in this context and provide concrete solutions for addressing some of the identified challenges.

ACKNOWLEDGEMENTS

This work has been partially supported by the GAUSS national research project (MIUR, PRIN2015, Contract2015KWREMX).

REFERENCES

Almutairi, A., Sarfraz, M., Basalamah, S., Aref, W., and Ghafoor, A. (2012). A distributed access control architecture for cloud computing. *IEEE software*, 29(2):36–44.

Arkoudas, K., Chadha, R., and Chiang, J. (2014). Sophisticated access control via smt and logical frameworks. *ACM Trans. Inf. Syst. Secur.*, 16(4):17:1–17:31.

Ausanka-Crues, R. (2001). Methods for access control: advances and limitations. *Harvey Mudd College*, 301:20.

Bertolino, A., Busch, M., Daoudagh, S., Lonetti, F., and Marchetti, E. (2014a). A toolchain for designing and testing access control policies. In *Engineering Secure Future Internet Services and Systems: Current Research*, pages 266–286.

Bertolino, A., Daoudagh, S., Lonetti, F., and Marchetti, E. (2016). Testing access control policies against intended access rights. In *Proceedings of the 31st Annual*

ACM Symposium on Applied Computing, Pisa, Italy, April 4-8, 2016, pages 1641–1647.

Bertolino, A., Daoudagh, S., Lonetti, F., Marchetti, E., Martinelli, F., and Mori, P. (2014b). Testing of polpa-based usage control systems. *Software Quality Journal*, 22(2):241–271.

Bertolino, A., Daoudagh, S., Lonetti, F., Marchetti, E., and Schilders, L. (2013). Automated testing of extensible access control markup language-based access control systems. *IET Software*, 7(4):203–212.

Bertolino, A., Traon, L., Lonetti, F., Marchetti, E., and Mouelhi, T. (2014c). Validation of access control systems. In *Engineering Secure Future Internet Services and Systems - Current Research*, pages 210–233.

Cai, F., Zhu, N., He, J., Mu, P., Li, W., and Yu, Y. (2018). Survey of access control models and technologies for cloud computing. *Cluster Computing*, pages 1–12.

Calabrò, A., Lonetti, F., and Marchetti, E. (2018). Monitoring of access control policy for refinement and improvements. In *Proc. of Software Quality: Methods and Tools for Better Software and Systems*, pages 17–36.

Hu, V. C., Kuhn, D. R., Xie, T., and Hwang, J. (2011). Model checking for verification of mandatory access control models and properties. *International Journal of Software Engineering and Knowledge Engineering*, 21(01):103–127.

Hwang, J., Xie, T., Hu, V., and Altunay, M. (2010). Acpt: A tool for modeling and verifying access control policies. In *Proc. of International Symposium on Policies for Distributed Systems and Networks*, pages 40–43.

Jin, X., Krishnan, R., and Sandhu, R. (2012). A unified attribute-based access control model covering dac, mac and rbac. In *IFIP Annual Conference on Data and Applications Security and Privacy*, pages 41–55.

Lonetti, F. and Marchetti, E. (2018). On-line tracing of XACML-based policycoverage criteria. *IET Software*.

Ma, Z., Yang, Y., and Wang, Y. (2015). A security policy description language for distributed policy self-management.

Margheri, A., Masi, M., Pugliese, R., and Tiezzi, F. (2017). A rigorous framework for specification, analysis and enforcement of access control policies. *IEEE Transactions on Software Engineering*.

Martinelli, F. and Matteucci, I. (2011). Preserving security properties under refinement. In *Proceedings of the 7th International Workshop on Software Engineering for Secure Systems*, SESS '11, pages 15–21.

OASIS (2005). eXtensible Access Control Markup Language (XACML) Version 2.0. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

Park, J. and Sandhu, R. (2002). Towards usage control models: beyond traditional access control. In *Proc. of the seventh ACM symposium on Access control models and technologies*, pages 57–64. ACM.

Rensink, A. and Gorrieri, R. (2001). Vertical implementation. *Information and Computation*, 170(1):95 – 133.

Sharma, P. K., Kaushik, P. S., Agarwal, P., Jain, P., Agarwal, S., and Dixit, K. (2017). Issues and challenges of data security in a cloud computing environment. In *Proc. of 8th Annual Conference on Ubiquitous Computing, Electronics and Mobile Communication*, pages 560–566.

Suhendra, V. (2011). A survey on access control deployment. In *International Conference on Security Technology*, pages 11–20. Springer.

Tianyi, Z., Weidong, L., and Jiaxing, S. (2011). An efficient role based access control system for cloud computing. In *11th International Conference on Computer and Information Technology*, pages 97–102.

Tsai, W.-T. and Shao, Q. (2011). Role-based access-control using reference ontology in clouds. In *Proc. of 10th International Symposium on Autonomous Decentralized Systems*, pages 121–128.

Ubale Swapnaja, A., Modani Dattatray, G., and Apte Sulabha, S. (2014). Analysis of DAC MAC RBAC Access Control based Models for Security. *International Journal of Computer Applications*, 104(5):6–13.

Veloudis, S., Paraskakis, I., Petsos, C., Verginadis, Y., Patiniotakis, I., and Mentzas, G. (2017). An ontological template for context expressions in attribute-based access control policies. In *Proc. of the 7th International Conference on Cloud Computing and Services Science*, pages 151–162.

Veloudis, S., Verginadis, Y., Patiniotakis, I., Paraskakis, I., and Mentzas, G. (2016). Context-aware security models for paas-enabled access control. In *Proc. of the 6th International Conference on Cloud Computing and Services Science*, pages 202–212.

Wang, W., Han, J., Song, M., and Wang, X. (2011). The design of a trust and role based access control model in cloud computing. In *Proc. of 6th International Conference on Pervasive Computing and Applications*, pages 330–334.

Weimer, D. L. and Vining, A. R. (2017). *Policy analysis: Concepts and practice*. Taylor & Francis.

Youniand Kifayat, K. and Merabti, M. (2014). An access control model for cloud computing. *Journal of Information Security and Applications*, 19(1):45–60.