A Survey on Access Control Mechanisms in E-commerce Environments

Christos Vasiliadis
University of Macedonia
156 Egnatia Str., 540 06
Thessaloniki, Greece
+30 2310 891706
vasiliadisc@uom.edu.gr

Christos K. Georgiadis
University of Macedonia
156 Egnatia Str., 540 06
Thessaloniki, Greece
+30 2310 891869
geor@uom.edu.gr

ABSTRACT
With continuously growing numbers of applications, enterprises face the problem of efficiently managing the assignment of access permissions to their users. Access Control (AC) represents the process of mediating every request to services and data, maintained by a system and determining whether the requests should be granted or denied. The AC decision is enforced by a mechanism implementing regulations established by a security policy. Different AC policies can be applied, corresponding to different criteria for defining what should, and what should not be allowed. Over the past few years AC mechanisms have been deployed in diverse enterprises of all sizes. The aforementioned success has led to an abundance of available access control models corresponding to the special needs of every enterprise. In this paper we firstly attempt to stress the importance for every business that uses information systems to incorporate access control mechanisms in its production line. In the framework of investigating the problem of AC, studies have been held on specific issues relating to the configuration and the management of AC methods. We comprehensively study and classify the problem properly discovering and selecting AC mechanisms by reviewing recent research results and secondly analyze and identify the current AC approaches along with its several variants and the corresponding solution strategies. We highlight the advantages, the methods and techniques involved and the challenges of each approach. Finally, we analyze their influence on designing and implementing these approaches in e-commerce environments, discuss the limitations of existing methods and identify new areas of research that can lead to further enrichment of this field.

Categories and Subject Descriptors
D.4.6 [**Operating Systems**]: Security and Protection-*Access control*

Keywords
Access control, business roles, role engineering, role mining, RBAC, ABAC, Usage Control, REBAC, cloud computing

1. INTRODUCTION
An important issue faced by administrators of computer systems, online and offline, and security analysts is to find appropriate mechanisms for access controls, mechanisms that their integration will help to maximize the benefits in a business environment.

Although several efforts have been made in the development of access control models for traditional database environments, the e-commerce environment is quite different from traditional one. In an e-commerce environment the resources to be protected are not only traditional data but also knowledge and expertise. For this purpose, the issue of finding and utilizing such access control mechanisms should be considered from a different perspective. A significant parameter that should be considered is the cost evaluation, i.e. the effort required for the administration and the functionality of the access control model the enterprise has incorporated [1,2]. Moreover, finding a suitable framework in which to apply real enterprise data that leads to optimization of access control mechanisms is another issue that deals strongly the scientific community.

A typical access control system includes subjects accessing objects through proper operations. The fundamental aim of access control, ie the principles and the high level guidelines concerning the design and administration of access control systems come from the system security policy, which is trying to give appropriate solutions in all recorded security requirements.

Systems that possess access control privileges are designed to maintain who can perform what, and who can have access to what resources [2,3,4]. In particular, for each IT system access control principles that regard the rights of subjects to objects must take place. Enterprises and organizations that use abundance of systems, have as primary purpose the protection of their resources. The problem becomes more complex if restrictions as the hierarchy in the organization are added.

It is widely accepted that there are not better or worse access control policies. This is because not all information systems have the same safety requirements. Hence, as an applicable general principle the policy choice depends on the individual characteristics of the environment to be protected [3]. There are three main types of access control policies, first is Discretionary access control (DAC), second is Mandatory access control (MAC) and the third is Role based access control (RBAC).

Discretionary access control (DAC), leaves the responsibility assignment and revocation of privileges at the discretion of individual users, who are called owners of the objects. In this policy, user has the complete authority over all the resources it owns and also determines the permissions for other users who have those resources. The restriction of access to the objects is based on the identity of subjects or the groups where they belong.

Mandatory access control (MAC) policies are used when a system contains information on a variety of classifications and there are users who are not authorized for the highest classification of the information contained in the system. Access

to information is limited by the principle of the necessary knowledge, so access to sensitive data is allowed only to those subjects that need to know such data to perform their tasks. The security policy administrator defines the usage of resources and their access policy and as model is commonly used in systems where confidentiality is the main priority.

Role based access control (RBAC). This policy is supported solely on defining roles from the permissions the users possess. As role is considered a set of rights, responsibilities and actions, related to a specific function of the enterprise. A role uniquely identifies a set of permissions, and users are assigned to appropriate roles based on their responsibilities and qualifications. The idea of matching rights/privileges throughout roles is quite old, but appeared for the first time in the works of Gligor and Sandhu [5,6]. The role-based models determine access by assigning users to one or more roles that have been created in the system based on the tasks they have to accomplish. Initially, support of roles of users was a part of DAC models as an access control approach since the role was purely faced as a whole, a user group. The situation changed with the advent of the formulation of role-based access control (RBAC). This model utilizes the ordinarily meaning of user role, which enhances through a strong formalism to combine additional features such as hierarchies and limitations [3].

In RBAC approaches, the granted or denied access decisions are based on the roles that individual users undertake within an enterprise. The process of defining roles is based on a detailed analysis of the tasks of the organization that have to be accomplished, including data from the widest possible range of users [6]. Roles are assigned to users based on qualifications they possess, they can easily be retrieved and new roles can be developed and assigned to users. The key task in deploying RBAC is to find suitable user-role assignments and role-permission assignments, in effect, define the appropriate set of roles. Assignment of a role to a user, is performed in such a way the user cannot get more benefits than what is necessary to accomplish his tasks [3,5]. RBAC has established itself as a well-accepted model for access control in many organizations and enterprises.

The process of defining roles in an enterprise is quite complex since various aspects have to be considered that will affect positively or negatively the functionality after integration of the access control model. An important concept that needs to be determined is that of cost. The definition of cost mainly refers to the effort required for the administration and functionality of the access control model that the organization has incorporated. Moreover, another important aspect is the creation of an access control mechanism framework that will apply real datasets from business environments and its results can be used for the optimization of the algorithms used for role creation. Such approaches have been proposed by Colantonio and other researchers using metrics that assess the roles either to their functionality or in their business meaning [2,4].

2. AUTHORIZATION POLICIES, ACCESS AND USAGE CONTROL

As numerous researchers have pointed out, there are issues that require further consideration. In this paper, studies in individual issues were conducted related to configuration and management of access control approaches. Major research directions of access control configurations are the following.

2.1 RBAC model extensions, role engineering and business meaning or roles

Despite the widespread adoption of RBAC oriented systems, enterprises frequently implement them without due consideration of required roles. To minimize deployment effort of the access control policy, organizations unconsciously neglect the process of defining roles in the initial part of the deployment project. It is very usual to define high level roles that do not reflect the actual organizational requirements. The results of this irrational process of role definition is that deployed systems do not yield the expected benefits. Additionally, it also leads to role misuse. The area of role engineering, i.e. the process of determining the required set of roles by combining several permissions, is facing such problems [2,5,7]. Once role definitions are established, there has no more slack to shift responsibilities or to demand additional permissions. Its aim is to properly customize RBAC systems in order to capture the needs and functions of the organizations.
Traditionally, role engineering was carried out in a top-down fashion wherein organizational business processes are analyzed and decomposed into smaller units. Once the permissions required to carry out specific tasks are identified, they can be grouped into appropriate functional roles. The process is repeated till all the job functions are covered. The top-down approach suffers from a major drawback, namely, scalability, when the number of business processes, users and permissions become very large. In recent years, an alternative bottom-up approach, termed role mining has been proposed [8]. It considers the existing user-permission assignments to define the roles using a process that can be automated. Thus, role mining uses data mining techniques to generate roles from the access control information of the systems. Current role mining approaches, however, must deal with some practical issues [2]:

Meaning or Roles. Automatically elicited roles often do not have any connection to business practice. Existing role mining approaches can be classified in two different classes [9]. The first class pursues to identify complete RBAC configurations, i.e. the minimal set of roles that cover all access rights. Such algorithms have been suggested by researchers as Colantonio who represented a variant of Apriori algorithm, the so called RBAM (Role-Based Association-rule Mining) algorithm [2]. Its aim is the recognition of the optimal set or roles, i.e. the set of roles with the minimum cost. To gain greater flexibility, a second class of algorithms proposes a complete list or roles, so role designers can manually select the most relevant ones [4,10].

Algorithm Performance. The problem of determining an optimal set of roles from the user-permission assignments to obtain a useful RBAC state is referred to as the Role Mining Problem (RPM). Several works have proved that the role mining problem can be reduced to many other NP-hard problems, such as binary matrix factorization, bi-clustering, graph vertex coloring to name a few.

Noise Within Data. The number of elicited roles that are created from the existing approaches is often very large due to noise within the data, namely, permissions exceptionally or accidentally granted or denied.

Problem Complexity. The introduction of new users, new permissions and relationships between them into the access control approach may require reassessing the role set that has been deployed. Hence, a complete redesign of the RBAC configuration is unavoidable in order to reduce the overall administration cost.

Risk of Unmanageable Roles. The trivially application of standard data mining approaches frequently yields roles that have no connection to business needs and functions. Thus, poorly

designed roles increase the risk of incorrectly authorized users [11].

On the question of the meaning of the roles, a promising approach on the design of a RBAC state is that of assigning a business meaning to roles. A role is likely to be meaningful from a business perspective when it involves activities (tasks) within the same business processes. To this aim, two different approaches are proposed [2,5]:

- The first introduces a new metric to assess how useful or not is a certain role from a business prospect. To evaluate roles usage of indices has been proposed to measure the spreading of these roles among the enterprise structure.

- The second approach includes a methodology where the dataset is decomposed into smaller subsets that are homogeneous from a business prospect. Deploying appropriate indices make it possible to locate the desired set of roles and permissions that are manageable by the same role, so it is viable to identify and choose the roles that fulfill the criteria of business meaning.

Finding the right solution strategies for the different variants of RPM is considered a complex process, therefore the classification of models corresponding to specific features deemed necessary. The top-level classification distinguishes between two classes of role mining models, namely,

- The Deterministic models and
- The Probabilistic models

The first class includes RMP approaches that aim to minimize a given metric, whereas second class casts RMP variants as an inference problem. The Deterministic model class, consists of four subclasses:

- General, considering the RMP approaches and the resulting RBAC configuration with a chosen optimization metric being minimized

- Constrained, dealing with role mining in the presence of one or more constrains

- Perturbation, aiming to derive RBAC states while taking into account the existing set of roles without altering the bounded number of roles.

- Extended, considering novel approaches to Boolean matrix decomposition that is used for RMP.

Similarly, the Probabilistic class can be subdivided in two subclasses:

- General, that casts RMP as an inference problem and

- Constrained, which includes approaches for enforcing certain cardinality constraints in the resulting RBAC state.

Significant contribution in the direction of studying the RMP and its variants offers the work of Kunz e.t. [4]. Researchers conducted a detailed investigation of relevant research efforts and present a variety of quality criteria for their roles. Such criteria are set out below, Achieve Completeness, Reduce Number of Roles, Decrease Role Set Similarity, Minimize Users/Permissions per Role and Minimize/Maximize Roles per User/Permission, Fulfill Role Constraints, Reduce of Weighted Structure Complexity (WSC), Increase Role Coverage [5].

2.2 Tools and data sets

Since the role mining process does not require any physical intervention by humans, a number of tools have been proposed that either directly perform role mining or aid the role mining process by determining several relevant factors. These tools, as support in the role definition process, prevent any sort of intentional or unintentional errors, making reliable the final configuration of the RBAC system. Several tools have been proposed, such as below:

ORCA. ORCA is a Java-based tool intended as an instrument to visualize the hierarchy of existing permissions and to support the transformation of the cluster hierarchy into an enterprise role. This tool performs role mining by grouping similar permissions assignments and creates a hierarchy of permission clusters [12].

RMiner. In RMiner we want to provide a tool set to help researchers or administrators do role engineering work. It is also a Java-based tool set that implements several role mining algorithms such as CompleteMiner, FastMiner, HierarchicalMiner, ORCA, StateMiner, GraphOptimization, Anto-apriori and WeightedRoleMining. It provides a framework to edit the role-based configurations obtained from these algorithms [13].

VAT (Visual Assessment of cluster Tendency). VAT is a tool for analyzing cluster tendency. Determining whether roles can be identified from a given User-Permission Assignment (UPA), the number of roles that can be identified, and whether partitioning can be performed on the UPA is called role tendency analysis. To use VAT for role engineering, a role definition tool, named RoleVAT, is proposed for the visual assessment of user and permission tendencies to establish practical need for RBAC. RoleVAT can be used on both users and permissions given the user permission assignments of an enterprise [14].

After the definition of role mining tools, one more aspect that has to be considered is their evaluation both in real as well as in synthetic datasets [15].

- *Real Datasets*. In the scientific community there is a set or nine real-world datasets that has been widely used for the assessment and performance evaluation of role mining algorithms. Among these, the most commonly used are the *apj*, *emea*, *americas small* and *americas large* [16].
- *Synthetic Datasets.* Besides using real datasets, assessment of the various role definition processes can be achieved via the use of synthetic datasets created using random data generators. The data generator takes as input the number of users, permissions and roles to generate a pair of user-role (UA) and permission-role (PA) assignments matrices. Combining these two matrices, the corresponding user-permission assignment (UPA) is obtained, which serves as the input to role mining algorithms [17].

2.3 Usage Control

The evolution of computing systems introduces new security requirements and therefore the need for new security mechanisms deemed necessary. Traditional access control solutions do not adequately respond to these new challenges addresses by modern computer systems and their policies, like the ones in e-commerce environments. Today, highly distributed and network connected computer environments require flexible and persistent mechanisms for protecting the access and usage of digital resources. *Usage control* (UCON) is a generalization of access control that extends authority not only to who may have access which data, but also to how the data may be distributed or used

afterwards. Traditionally, access control addresses only the approval decisions on a subject's access to targeted resources. *Obligations* are requirements that have to be met by the subjects to allow access while *conditions* constitute obligations that have to be fulfilled both by the subjects and by the objects and are independent form the environmental requirements that have to be satisfied in order to allow access [18]. As mentioned before, usage control generalizes access control by controlling the usage of data after their distribution. Therefore development of access control mechanisms that lead to the expression Usage Control (UCON) models seems to be necessary. The term *usage* means the use of the rights of digital objects while the term *control* includes both the rights for the exploitation of objects and the royalties for the authorization of such rights.

In today's highly dynamic, distributed environment, obligations and conditions constitute critical factors for optimum control of digital objects. Enterprises and organizations have to perpetually readjust their commerce environmental policies to encounter with mutability issues that come from the consecutive updates on subjects or objects attributes as a consequence of access to specific rights. When data providers release data, they would desire mechanisms on the user's side to enforce their restrictions. To this end, a UCON model to formalize the problem domain at a realistic level of complexity deemed necessary to incorporate by enterprises to maintain power of controlling data [19].

2.4 Attribute-Based Access Control (ABAC)

Contemporary approaches of access control combine concerns of control use, providing an environment in which application of the user/subject to perform operations on objects is approved or rejected based on the evaluation of object's and subject's attributes as well as on the environment's characteristics such as the hour, the day etc. Models of this type of access control recently gained momentum, due to the complexity of role based (RBAC) mechanisms [20,21,22].

The reasoning of this approach based on the perception that the policies of traditional access control do not fully meet the constantly changing needs and access requirements. In DAC models, information may be accessed by unauthorized users because once the information is acquired by a process, DAC do not have any control on the flow of information and can be copied from one object to another. On the other hand, MAC deals with information flow and gives solution to this problem by attaching security restrictions on both user's and object's access. However, the policies in DAC and MAC are fixed and no flexible to new imports. Moreover, RBAC mechanisms do not cover all the requirements encounter in real world scenarios, because it is difficult to implement the model in a constantly changing environment, so roles are assigned statically to the users. Another limitation of RBAC is that the permissions are referring to individual projects, so it is adequate in situations where a large number of objects exist and leads to role definition significant problem.

Consequently, a more general model, specifically attribute-based access control (ABAC), that encompasses the benefits of DAC, MAC, RBAC and UCON models, while at the same time exceeds their limitations deemed necessary to be composed. ABAC is considered more flexible compared to RBAC, since it can easily facilitate contextual attributes as access control parameters.

The term attribute refers to a property that can be expressed as a name:value for each entity of the system, like subjects, objects, even the environment itself to provide authorizations. Any additional features can be integrated within the same framework of the model so that it is possible to import new attributes to the existing framework [2,21].

Enterprises are based on influential access control mechanisms to ensure that corporate resources (applications, products, data) are not exposed to anyone other than authorized users. As requirements consecutive change, flexible access control mechanisms are necessary to adapt to these needs. The appliance of access control policies based on attributes allow enterprises to address simultaneously a variety of issues necessarily for the functionality, increasing productivity and remaining sensitive to security matters [20,21].

3. RECENT METHODS

3.1 Attributes and cloud computing

Cloud computing is a new computing model that provides services and access to resources stored on distributed service-oriented architecture called cloud. A growing number of enterprises utilize cloud computing as technological infrastructure because it provides efficient data storage, resource sharing and services in a distributed manner with great ease.

Benefits of using cloud computing involve reduced cost, better operation facilities and increased efficiency in sharing data. However, a growing concern in the adoption of cloud infrastructure as a service (IaaS), is arising due to the security and privacy of the sensitive data that are shared under third party cloud service providers. Therefore, access to sensitive data should be granted under certain restrictions that could be considered as attributes of an ABAC model. Such mechanisms work with identification, authentication and authorization, so for cloud computing infrastructures are appropriate since they are secure, flexible and scalable [21,22].

3.2 Attributes and social networks-Relationship Based Access Control (REBAC)

Online social network (OSNs) have attracted a large amount of users that regularly interact each other and share information and data for various purposes. In such cases, access control policies are characterized by the interpersonal relationships among users and the access control mechanisms are known as Relationship-Based Access Control (REBAC) models. On OSNs where access to data is greatly influenced by the relationships among users, the composition of self-adaptive mechanisms based on these specific characteristic and requirements deemed necessary for their proper functioning.

Specifically, access control based on relationships has been adopted as the most significant approach to monitor access on social networks, where administrators of these networks can delimit authorization policies, based on relationships of users with other ones without the obligation of knowledge of the domain name of users of their networks [23,24].

Additionally, the use of relationships is several times not capable of imposing security and privacy policies. And these are restrictions necessary for the proper functioning of every social network. Thus, one solution strategy to this problem is the development of a mechanism that unifies access control policies based on attributes and utilize them to ReBAC models.

The access control policies based on relationships, recently began to generalize in order to be appropriate for incorporation in business environments. The motivation for the development of a general ReBAC model is that the mechanisms controlling access based on attributes (ABAC) are not appropriate to express policies that depend on relationships involving entities beyond the scope

and purpose of the request for access, especially when such entities are determined by a sequence of relationships and differences in attributes [25].

3.3 Discussion

Access control in information systems ensures that actions to the system objects/resources occur according to the modes fixed by the corresponding security policies. A security policy is expressed by access rules, which regulate how authorization decisions are determined. In addition to the two major categories of access control models (discretionary and mandatory), role-based models are widely used, as their policy-neutral nature allow them to support both discretionary and mandatory functions. Substantial research on role engineering/role mining has been published, and the importance of context has been recognized as a decisive factor to flexibly express application-level conditions. Context-awareness offers a variety of dynamic parameters, set to be used during the runtime in order to control in a fine-grained way the activation of user permissions.

However, in modern computing environments crucial required configurations, such as the assignment of users/permissions to roles and the role design and engineering is difficult and burdensome. Usage control and trust concepts, privacy concerns in Web-based and mainly in mobile platforms, cloud/Web services demanding requirements and social networks' relationship-based approaches are some characteristic indications of the growing need for a more general access control model. Attribute-based access control is increasingly appreciated as a viable solution to this direction, covering discretionary, mandatory and role-based models. An attribute is a property expressed as a name:value pair associated with any entity in the system, including users, subjects, objects, actions, context parameters and policy elements (such as roles, access control lists, security labels, etc.). It seems that a mature authorization mechanism, matching the needs of emerging technologies, has to effectively manage an extensible framework of attributes.

4. CONCLUSIONS - FUTURE WORK

This paper presents access control approaches, especially those which can be evaluated with policies of role mining algorithms and those that encompass benefits and exceed limitations of these approaches. We try to demonstrate the effectiveness of adopting models based on attributes and relationships because of their ability to meet the requirements that constantly change in e-commerce business environments.

Directions of future work in the context of access control approaches include:

- Development of new approaches and evolution of existing which are intended to identify the optimal set of roles, in other words the one with the minimum administration cost. New metrics can also be created to evaluate the functionality of roles in their business perspective.
- Design of access control methods by adopting the philosophy of ABAC. Role quality criteria will be explored based on their attributes. Datasets and tools studied within the role extraction process will be used to create feature-based approaches that fully meet the constantly changing needs and requirements for obtaining access to e-commerce environments. For the successful implementation of ABAC approaches, policies and restrictions of these models must be properly identified.
- Development of case studies, where the above approaches are intended to improve the access control methods in e-commerce environments. Through these case studies, these approaches (Business RBAC mining and ABAC-oriented) using relative roles mining tools will be evaluated, mainly on synthetic data (and on real data if it becomes possible).

5. REFERENCES

[1] De Capitani Di Vimercati, S., Foresti, S., Samarati, P., Jajodia, S. 2007. Access control policies and languages. *International Journal of Computational Science and Engineering*, 3(2), 94-102.

[2] Colantonio, A. 2011 Role mining techniques to improve RBAC administration, *Ph.D. Thesis*, Universita degli Studi 'Roma Tre'

[3] Georgiadis, C. 2016. Web technologies and e-commerce: Current Trends and Challenges (in Greek), ISBN 978-960-603-125-0

[4] Alessandro, C., Di Pietro, R., Alberto, O. 2011. Role mining in business: (Taming Role-Based Access Control Administration).

[5] Kunz, M., Fuchs, L., Netter, M., Pernul, G. 2015. How to Discover High-Quality Roles? A Survey and Dependency Analysis of Quality Criteria in Role Mining. *In International Conference on Information Systems Security and Privacy* (pp. 49-67). Springer International Publishing.

[6] American National Standards Institute (ANSI) and International Committee for Information Technology Standards, Information Technology-Role Based Access Control, ANSI/INCITS 359-2004.

[7] Coyne, E. J. 1996. Role engineering. *In Proceedings of the first ACM Workshop on Role-based access control* (p. 4). ACM.

[8] Frank, M., Buhmann, J. M., Basin, D. 2010. On the definition of role mining. *In Proceedings of the 15th ACM symposium on Access control models and technologies* (pp. 35-44). ACM.

[9] Molloy, I., Chen, H., Li, T., Wang, Q., Li, N., Bertino, E., ... Lobo, J. 2008. Mining roles with semantic meanings. *In Proceedings of the 13th ACM symposium on Access control models and technologies* (pp. 21-30). ACM.

[10] Vaidya, J., Atluri, V., Warner, J. 2006. RoleMiner: mining roles using subset enumeration. *In Proceedings of the 13th ACM conference on Computer and communications security* (pp. 144-153). ACM.

[11] Celikel, E., Kantarcioglu, M., Thuraisingham, B., Bertino, E. 2009. A risk management approach to RBAC. *Risk and Decision Analysis*, 1(2): 21–33.

[12] Schlegelmilch, J., Steffens, U. 2005. Role mining with ORCA. *In Proceedings of the tenth ACM symposium on Access control models and technologies* (pp. 168-176). ACM.

[13] Li, R., Li, H., Wang, W., Ma, X., Gu, X. 2013. RMiner: a tool set for role mining. *In Proceedings of the 18th ACM*

symposium on Access control models and technologies (pp. 193-196). ACM.

[14] Wang, L., Geng, X., Bezdek, J., Leckie, C., Kotagiri, R. 2008. SpecVAT: Enhanced visual cluster analysis. *In Data Mining, 2008. ICDM'08. Eighth IEEE International Conference on* (pp. 638-647). IEEE.

[15] Mitra, B., Sural, S., Vaidya, J., Atluri, V. 2016. A Survey of Role Mining. *ACM Computing Surveys (CSUR)*, 48(4), 50.

[16] Ene, A., Horne, W., Milosavljevic, N., Rao, P., Schreiber, R., Tarjan, R. E. 2008. Fast exact and heuristic methods for role minimization problems. *In Proceedings of the 13th ACM symposium on Access control models and technologies* (pp. 1-10). ACM.

[17] Vaidya, J., Atluri, V., Warner, J., Guo, Q. 2010. Role engineering via prioritized subset enumeration. *IEEE Transactions on Dependable and Secure Computing*, 7(3), 300-314.

[18] Pretschner, A., Hilty, M., Schütz, F., Schaefer, C., Walter, T. 2008. Usage control enforcement: Present and future. *IEEE Security & Privacy*, 6(4).

[19] Pretschner, A., Hilty, M., Basin, D., Schaefer, C., Walter, T. 2008. Mechanisms for usage control. *In Proceedings of the 2008 ACM symposium on Information, computer and communications security* (pp. 240-244). ACM.

[20] Hu, V. C., Kuhn, D. R., Ferraiolo, D. F. 2015. Attribute-based access control. *Computer*, 48(2), 85-88.

[21] Fisher, W., Brickman, N., et al. 2016. Attribute based access control, NIST Cybersecurity Practice Guide, NIST Special Publication 1800-3c (draft).

[22] Sandhu, R. 2015. Attribute-Based Access Control Models and Beyond. *In ASIACCS* (p. 677).

[23] Fong, P. W. 2011. Relationship-based access control: protection model and policy language. *In Proceedings of the first ACM conference on Data and application security and privacy* (pp. 191-202). ACM.

[24] Cheng, Y., Park, J., Sandhu, R. 2012. Relationship-based access control for online social networks: Beyond user-to-user relationships. *In Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Conference on Social Computing (SocialCom)* (pp. 646-655). IEEE

[25] Stoller, S. D. 2015. An administrative model for relationship-based access control. *In IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 53-68). Springer International Publishing.