ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

Identity and Access Management

Naveen Pratiksha[1], Prof. S. G. Raghavendra Prasad[2], Dr. Jitendranath Mungara[3]
M.Tech Student[1], Assistant Professor[2], HOD[3]
Department of Information Science and Engineering[1, 2, 3]
R V College of Engineering, Bangalore, India[1, 2]
New Horizon College of Engineering, Bangalore, India[3]

Abstract:
Various Identity and Access Management (IAM) architectural challenges are emerging for the effective deployment of applications in digital entitlement context. Data Management solutions should incorporate efficient access control techniques and adopt an optimal setup among countless and complex approaches in providing access control services. Web Single Sign-on (SSO), federated identities, password synchronization and service granularity can be accomplished through the IAM capabilities, so that System can address and fulfill most of the contemporary access management challenges. Our work proposes an innovative model to manage the multilevel integration of identity, authentication and authorization modules based on formal policy-based methods and various access control mechanisms in order to provide secure access to the resources. In the proposed model, we analyze and integrate identity, authentication, user roles, authorization access control levels, and rule validation mechanisms. Finally, the model offers policy-based and integration capabilities enabling automated controls, improved efficiency and simplified management.

Keywords: components: Identity and Access Management, RBAC, hierarchical access control, SOA

I. INTRODUCTION

Currently, most of the pioneering advanced business applications are deployed by leverage resolution frameworks which support the service-oriented architecture (SOA) model to respond more quickly to the rising internet activities and to the speedily ever-changing demands. Many paradigms of SOA applications are present in distributed, decentralized and grid-based heterogeneous environments. For example, cloud computing, that has already gained popularity with the aim to cut back Capex and Opex prices, is taking advantage of SOA by providing the resources as services. However, within the case of cloud computing wherever data owners and cloud service supplier aren’t within the same trusted domain, there seem many security and access management issues. Parallel to their efforts to stay up with the continual developments and enhancements in technology, organizations frequently explore and deploy subtle identity, authentication and authorization capabilities (i.e. trust and federation, delegated identity management, password management, and multi-domain access) planning to offer secure access to network and system resources. Till recently, thanks to the increased overhead and security complexness in decision-making for user access management solutions, most of the Identity and Access Management (IAM) tasks were assigned to the application developers, the network engineers and the security officers, who most often had little knowledge about the service processes and needs. As a typical example, some of these tasks can be related to access requests to grant or revoke access to protected resources during any Join/Move/Leave (JML) activity in the organization. This paper specifically presents an innovative policy-based model for SOA, and addresses the associated access control needs. The proposed solution integrates the IAM methods with an effective policy-based SOA management by analyzing the IAM methods used by the application delivery platform and the service management disciplines, when accessing identity data and supporting identity life cycle processes.

The rest of this paper is organized as follows. In sections 2 and 3, we present a review of the literature and the necessary preliminaries in the context of access control management for SOA. Section 4 describes the conceptual overview of the proposed model. Then, we provide the evaluation of this model in section 5. We summarize our results and conclude the paper in section 6.

2 RELATED WORK

The Discretionary Access Control (DAC) model and the Mandatory Access Control (MAC) model, the earliest access control models, have served as the precursors for the Role-Based Access Control (RBAC) models [1]. While DAC models depend on access control lists (ACLs) for determining authorization, the MAC models are typically designed using the concept of information flow control and they perform specific operations on the object or the target. Numerous later models, like the multi-level access control models, have evolved to facilitate the implementation of different security contexts, provide the capabilities for defining the necessary access control policies and ensuring to appropriate security levels. RBAC can be considered as a combination of mandatory and discretionary access control models [2]. RBAC is based on separate roles for relevant sets. RBAC provides greater flexibility as the users can be assigned several roles, thus most of the current commercial access control solutions follow RBAC. With the purpose of augmenting the hierarchical interference of user attributes, the Attribute Based Access Control (ABAC) can be imposed to assign the appropriate permissions to the user, and provide access to the Resources, regardless of the need for appropriate constraint specification and enforcement mechanisms [3]. Typically, DAC is very efficient in letting users of an online social network choose who may access their data, while MAC can be used to get access to the top-secret documents in high security requirement implementations. In RBAC implementations, the user gets access to the application with different levels of permissions. For instance, an employee working for Human-Resources (HR) can be authorized and granted the fitting role to work in the HR application to perform her duties. Contrary to this, in the case of ABAC, the HR employee gets access to the payroll sub-system and not to the rest of the HR components, because of her payroll accountant profile and atomic-valued attributes. Apart from the traditional access control models, a lot of research has been conducted in the past to incorporate fine-grained access-control (FGAC) [4] or coarse grained access-control (CGAC) techniques. The User Based Access Control (UBAC) model, the Usage Control Model (UCON) and the ABAC Temporal Based Access Control model (TBAC) are proposed variations of the original access control models, and arise various security concerns in the delivery of SOA or cloud-based solutions. In the case of SOA, several protocols and data formats can be used in cross-domain implementations. In cloud-based implementations, there might exist multiple cloud-service providers, where each one can issue or change the attributes independently. Thus, there is no trusted and closed environment in which we may be competent to apply solely the traditional access control models.

The distributed RBAC (dRBAC) [5], which supports large distributed systems and multiple organization access - when necessary, aims to reduce the authorization loads by using global roles across distributed systems along with local roles for each one of them. Thus, it is appropriate to give access control to resources across multi-domains and cloud environments. The Temporal Role-Based Access Control (TRBAC) model [6] introduces the concept of role triggers and supports temporal dependencies. These actions allow the periodic or time-based role assignments and removals to get access to the resources, and provide greater flexibility, granularity, prioritization and consistency checks capabilities. However, it cannot manage several temporal variables such as the constraints on the user-roles and the role-permission assignments. Generalized Temporal Role-Based Access Control (TRBAC) models [7] and XML-based X-GTRBAC [8] are proposed to improve the context-aware dynamic access control requirements and the control capability on temporal constraints. Several other variations of TRBAC have evolved to solve the problems with the role activation event conflicts, when the constraints are violated [9]. The cloud-optimized RBAC (coRBAC) access control is a cloud-enabled model that improves the authentication time for large number of users across multi-domain environments [10], since in large-scale enterprise or cloud-computing environments role maintenance requires substantial amounts of time and space. As most of the aforementioned models can handle the files but not the content, Multi-Role Based Access Control (MRBAC) for distributed multimedia systems [11] have been proposed. Recent works [12] provide techniques for creating a policy-compliant service composition through a graph, as well as the evaluation of policies [13] during service compositions and multi-level security classes of information flows [14] for cloud-based solutions. In conclusion, although the RBAC models have been analyzed and utilized extensively as the dominant access control models, they require an efficient and constructive organizational policy, and a hierarchical role-based approach. RBAC also lacks of temporal capabilities, and dynamic key management. In this vein, hierarchical access control models [15] have evolved. To the best of our knowledge, we have identified that these access control models do not have the necessary integration capabilities on how to manage horizontally certain authentication and authorization issues in complex, evolving, and dynamic environments (e.g. cloud-computing services). We have also identified the necessity for the existence of policy-based management that can enforce the appropriate access control rules with policy-based compliant services. Finally, we need to validate the effectiveness of the policy-sets in use, resolve any conflicts, tackle policy-violations, and ensure the end-to-end authorization flows and identity assertions. In the following section, we identify and present the access control needs and limitations, and then we propose the model and its integrated components.

3 IAM REQUIREMENTS FOR SOA APPLICATIONS

Several studies [16] have reported access management issues and inconsistencies in managing identities and services, such as duplication of identity and role information across the business processes, lack of identity data aggregation and increased complexity in SOA design [17]. Complexity produces configuration and management overhead (e.g. repetitive tasks for the account and authorization management), and results in higher administrative costs along with reduced usability. These are common complications for the deployment of SOA applications. With the aim to ensure a high assurance in the provision of IAM implementations, the appropriate access control policies need to be validated and enforced. In the literature [18], several frameworks have been analyzed and proposed to enforce an end-to-end access control model over web applications. In these proposals, the access model decision depends not only on the user intentions, the rule sets, the group memberships and the user attributes, but also on the enterprise architecture, the cross-domain deployments, the distributed environments, the trust model and the authorization challenges for each access control system. Among several others, granularity, manageability, delegation, revocation and composition are critical success access control factors [19]. A formal access-control policy language must be utilized to describe how to evaluate access requests in compliance with the policy rules, and then to provide real-time admission policy decisions [20]. Mazzoleni et al. [21] express the need to introduce a policy language for policy integration and for transferring dynamic security context. A standardized policy language facilitates the interoperability between policy control implementations and addresses policy-compliant services. Due to the higher integration of SOA applications, and the increased interest in cloud infrastructure solutions (i.e. SaaS) and in mobility, the access control services should adopt the latest IAM advancements, such as the utilization of federated identity management to establish logical links between the identities and the services in a secure way. Based on the above shortcomings, this paper proposes an innovative model based on formal policy-based methods and access control mechanisms. This model incorporates Policy-Based Management (PBM) practices and IAM capabilities to facilitate the access control management with the respective policies, and realizes a holistic policy-based access control approach described in the following sections.

4 PROPOSED INTEGRATION MODEL

As SOA necessitates common terminology and semantic, syntactic, technical and legal interoperability, the proposed model incorporates the idea of policy-based management access control rules. The orchestration of the access control components for the deployment of SOA is depicted in Figure 1. The proposed system secures the data exchange in the information retrieval and minimizes the security false positives. The model needs to ensure a high level of assurance and to avoid needs or any unambiguously specified (regulatory or systemic) policies. The security and policy assurance, the conformance to compliance, and the enforcement of the policies are achieved by using standard policy-based management components [22]. The proposed model (hereinafter referred to as IARAR) consolidates and maintains authentication, roles and authorization policies. IARAR incorporates an identity policy module, an authentication policy module, a role policy and an authorization policy module. In the current study, we analyze the management of these policies, and the integration of the respective modules aiming to achieve a holistic policy-based access control model. The detailed overview of IARAR is depicted in Figure 2. The illustrated integrated components are common management services, independent of the service delivery platform and the service administration. Regarding the access and policy management procedures, the model includes an Identity Service Engine (ISE), which is a security policy management and control platform that manages identity policies in a service domain. IARAR also introduces the Authentication Service Engine (AuthNSE) for authentication purposes, which provides various API interactions with the applications. The Role Mapping Engine (RME) defines the roles that provide the appropriate access-rights and permissions, and maintains the role memberships.

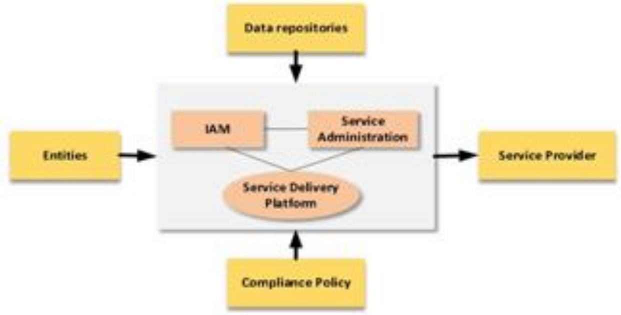

Figure 1. Access control model for SOA

The model also incorporates the Authorization Service Engine (AuthZSE) for access control and authorization needs to grant the required permissions to data and resources. Finally, the Rule Validator ensures policy conformance by performing the appropriate validation controls and policy rule checks, and then resolves any policy conflict.

4.1.1 Identity Service Engine (ISE)

ISE facilitates the identity data flows required for authentication, authorization and accounting operations. Upon receiving a request from an entity, ISE examines the identity data, such as the subject and the profile types, the resources and the identity attributes. The profiles associate the users and the groups with a set of data that describe their characteristics. In the case of cloud computing, we need to cope with security threats, such as data loss, data leakage and unauthorized access to protected resources. Besides, several risks in identity and account management emerge related to the legal ownership of data complications, the lack of interoperability among the systems, the existence of multiple proprietary protocols, and the complicated application of specific identity management work streams. Therefore, it is crucial to identify the risk event types and mitigate them by enforcing a strong authentication framework against stolen identities, leaked credentials, or infected devices.

4.1.2 Authentication Service Engine (AuthNSE)

The Authentication Service Engine (AuthNSE) receives the access requests from ISE and enforces the appropriate authentication policies by analyzing and applying the policy subjects, constraints and actions. These authentication policies can be statically preconfigured or dynamic [23]. The access request is then redirected to the Identity Provider (IdP) for validating the credentials. We need to enhance the security model by considering the use of secure communication protocols, maintaining and sharing directory information, and adapting strong or multi-factor authentication options. Special restrictions could be set by the service provider or the identity provider to conform to any exceptional and specific regulatory requirements, such as in the case of healthcare and data privacy of the patients.

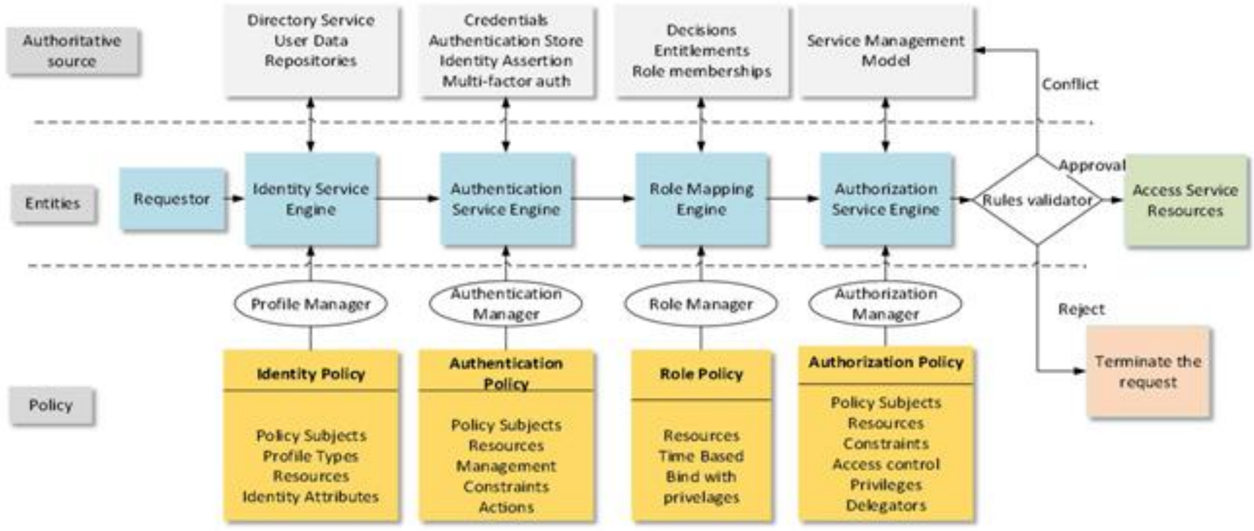

Figure. 2. The IARAR model

Additional privacy and security constraints (i.e. mandatory protected transport-layer connections, data integrity, auditability for fine-grained user access, and strong authentication mechanisms and separation of user management authentication with application access) also affect the authentication service implementation and integration.

4.1.3 Role Mapping Engine (RME)

We also need to define a set of permissions, roles and policy criteria in advance through the Role Mapping Engine (RME).

Then, we may be competent to evaluate and authorize an identity assertion from the IdP. In this context, the policy exchange messages can be formulated by using a standardized policy language. The policies need to address the association of roles with the resources, the hierarchy and the management of resources with the access control management. The role policy making engine is integrated with RME and the role manager of RME controls the assigned roles to the subjects based on specific attributes (e.g. organization user manager) and conditions (e.g. expiry date). For instance, RME determines the contractor's temporary data analysis access to a system component for a limited time and restrict access to another resource. In this scenario, the policy defines the role and the combined permissions of the subject, the authorized sessions to access the resources, and the access control conditions in the enterprise or organizational policy. RME determines whether the role policy is evaluated and applied based on the role memberships, the entitlements and the decisions in each context. Various complications could be encountered during the definition of the policies in terms of the semantic and the syntactic consistency. In this regard, we need to verify the validity of the policies, and ensure the policy enforcement along with the conformance and the policy constraints. **Authorization Service Engine**

(AuthZSE)

Upon receiving a request, AuthZSE applies the appropriate access controls, which incorporate the policy subjects, the resources, the actions, and the authorizations. The authorization policy sets define the actions and the privileges of an entity on the resources. This brings forth numerous security and operational issues related to the delegation procedures, the secure access management of shared resources, data confidentiality, system dependencies, integration limitations with SOA and several other burdens. The goal is to provide access to the target resource or service only to authorized entities that undertake specific duties. The access control policy management models may have different policy support capabilities and administration mechanisms. The access control service should define the application-level operations with the access policy rules based on the access criteria (i.e. sensitivity classification) and the infrastructure constraints (i.e. heterogeneity, cloud computing platforms, technology limitations), while the operational constraints are governed by the access admission policy decisions rules. In principle, SOA context should be decoupled from the authorization policy and the associated decisions. The authorization policy must be defined in the XACML policy document and retrieved on-demand during an authorization request.

4.1.5 Rule validator

Due to the existence of numerous policies from multiple sources, it is highly likely that we will encounter difficulties in deploying and implementing the appropriate policy decisions. Hence, the proposed model introduces a policy rule validator to prevent any contradicting requirements, detect access rights conflicts and resolve any policy violations. The rule validator monitors the system and assesses the privileges, the roles and the resources and report any deficiencies and violations. The access control remediation mechanism resolves any conflicts in the case of violations and misconfigurations, but the mechanism does not resolve fraudulent or negligent activities. In the case of violation, the system introduces a remediation indicator to provide a better view, whether this is a real conflict or not. If the problem is real, then the validator is expected to provide a high value to the indicator. Otherwise, the indicator gets a low value. Any conflict and violation is resolved within the review process by the rule validator. Still, we need an extensive use of service policies and hierarchical resources to detect and cope with any policy violations.

5 EXPERIMENTAL RESULTS

The evaluation of the proposed model is based on the access control authorizations' accuracy. The authorization request results may vary depending on the authorizations. When granting the appropriate permissions, and assigning the appropriate levels of authorizations we receive Correct Authorizations (COR), otherwise in the case of inappropriate access levels or mistaken policy decisions we get Mistaken Authorizations (MIS). Besides, we may also encounter Lack of Authorizations (LCK) cases, when there is a lack of automation ending up in manual intervention and provisioning. Apart from these types of authorizations, we have also considered the dynamic Running Costs (RNC) along with the Fixed Setup Costs (FSC) during the model simulations. In our study, we rely on repeated random sampling to obtain numerical results and we perform Monte Carlo experiments [24], as the repeated simulations generate statistically relevant outcomes. We perform statistical sampling and simulations to estimate the uncertainties and support the policy-based access control processes. In this context, Casassa et al [25] explore the associated policy decision processes for user account provisioning, and demonstrate how the system modelling and simulation activities can predict the impact of specific policies. Therefore, in the current paper, we complement the modelling and simulation regarding the policy decisions processes for authorizations instead. In the following simulations, we use Monte Carlo methods with nominal and parameterized input values for policy-based authorizations. The first scenario (Case #1) provides the modelling and prediction statistics for a standard access control system and the second one (Case #2) for the proposed model with the proposed model and the integrated modules. Table 1 provides the simulation data points for the accuracy efficiency of the correct authorizations over the total number of authorizations.

Table .1. Nominal authorization & cost values

Auth.types/ costs	**Case #1 Standard model**	**Case #2 IARAR model**
COR authZ	100	100
MIS authZ	10	5
LCK authZ	5	0
RNC	10	2
FSC	40	180

In our results, we rely on repeated random sampling that generate statistically relevant outcomes, and on simulations to estimate the uncertainties to support the policy-based access control processes. During the simulations, we obtained 5000 simulated observations to compare the two models and their respective statistics. Experiments can be reconfigured in a straightforward way by changing the simulated time frame and/or the number of times a model needs to be executed. Although the accuracy efficiency varies based on the uncertainty of values, we can estimate the cumulative probability depicted in (Figure 3).

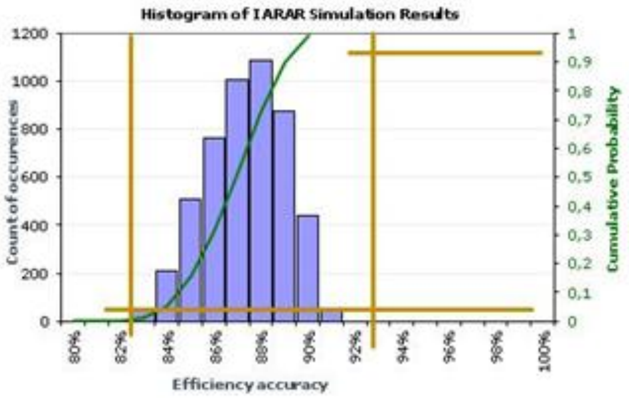

Figure .3. Statistical analysis of case #1

The analysis of the accuracy efficiency of introducing policies and the above-mentioned integrated service modules is depicted in Figure 4.

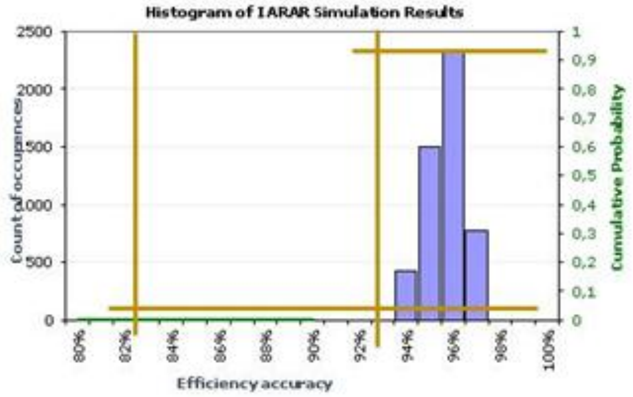

Figure .4. Statistical analysis of case #2

These simulations produce statistically significant low-level measures and related high-level metrics. By introducing more fine-grained access control policies in the policy engine and by considering more granular automation workflows, we can affect the access control authorizations positively, and to improve the accuracy efficiency and performance. The efficiency and the performance improvement for case #2 are presented in Figure 5.

6 DISCUSSION AND FUTURE WORK

IAM services are the essential building blocks in realizing an efficient SOA architecture. Various papers have addressed the identification, authentication, roles and authorization management, but in this paper, we presented

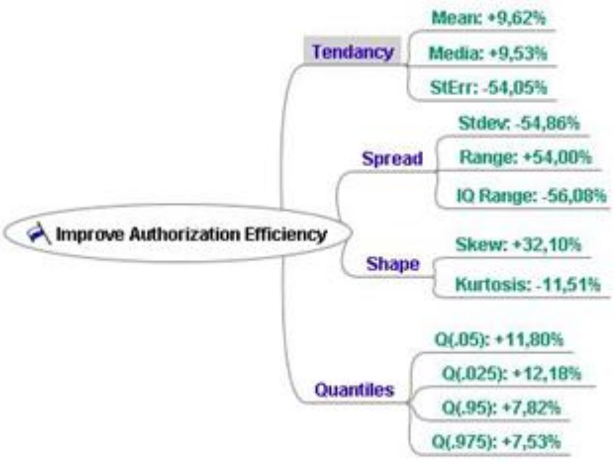

Figure .5. Comparison of statistics for case #1 vs. case #2

A consolidated model to integrate these access control components and showed how policy-based management can be enforced to apply the appropriate policy decisions. The proposed model is an inclusive PBM access control model, which includes identity, authentication, user roles, authorization access control levels, and incorporates rule validation mechanisms for each policy set. The support of policy-based and integration capabilities offers automated maintenance of the policy sets and controls, improved efficiency, simplified management, and support of different types of environment (e.g. enterprise, service provider). The proposed model supports further complex resource management extensions (i.e. optimal predictive resource allocation, resource usage, SOA performance, dynamic relocation of workloads), authorization capabilities (i.e. permission classes, task flows, SSO functionality, SAML and XACML uses in complex authorization scenarios), and policy and context management additions in SOA environment. Further experiments can assess external user data repositories, SAML providers and federated identity solutions. As cloud computing evolves and delivers new technologies and opportunities in reducing costs and ensuring better results in identity and access compliance, our future work will also focus on further enhancements in the cloud computing era.

7. ACKNOWLEDGMENT

This work has been partly supported by the University of Piraeus Research Center (UPRC).

8. REFERENCES

[1].A.V.D.M. Kayem, S.G. Akl, and P. Martin, “Adaptive Cryptographic Access Control”, Advances in Information Security, Springer, 2010, vol.48.

[2].D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, and R. Chandramouli, “Proposed NIST Standard for Role-Based Access Control,” ACM Transactions on Information and System Security, 2001, vol. 4, pp. 224 – 274.

[3].K. Bijon, R. Krishnan, and R. Sandhu, “Constraints Specification in Attribute Based Access Control,” IEEE/ASE Science Journal, 2013, vol. 2, no. 3, pp. 131-144.

[4].B. Hicks, S. Rueda, D. King, T. Moyer, J. Schiffman, Y. Sreenivasan, P. McDaniel, and T. Jaeger, “An architecture for enforcing end-to- end access control over web applications,” 15th ACM Symposium on Access Control Models and Technologies, 2010, pp. 163–172.

[5].E. Freudenthal, T. Pesin, L. Port, E. Keenan, and V. Karamcheti, “dRBAC: distributed role-based access control for dynamic coalition environments,” 22nd IEEE international conference on distributed computing systems, 2002, pp. 411-420.

[6].E. Bertino, P. A. Bonatti, and E. Ferrari, “TRBAC: A Temporal Role-Based Access Control Model,” ACM Transactions on Information and System Security, 2001, vol. 4, no. 3, pp. 191–233.

[7].J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, “Generalized Temporal Role Based Access Control Model,” IEEE Transactions on Knowledge and Data Engineering, 2005, vol. 7, issue 1, pp. 4–23.

[8].R. Bhatti, J. B. D. Joshi, E. Bertino, and A. Ghafoor, “X-GTRBAC: An XML-based Policy Specification Framework and Architecture for Enterprise-Wide Access Control,” ACM Transactions on Information and System Security, 2005, vol. 8, no. 2, pp. 187–227.

[9].M. Liu, and X. Wang, “Safeness Discussions on TRBAC and GTRBAC Model and an Improved Temporal Role - Based Access Control Mode”, International Journal of Security and Its Applications, 2015, vol.9, no.8, pp.23-34.

[10].Z. Tiayni, L. Weidong, and S. Jiaxing, “An Efficient role based access control system for cloud computing,” 11th IEEE International Conference on Computer and Information Technology, 2011, pp. 97-102.

[11].N. Zhao, M. Chen, S. Chen, and M. Shyu, “MRBAC: Hierarchical Role Management and Security Access Control for Distributed Multimedia Systems,” Proceedings of IEEE International Symposium on Object/Component/Service-oriented Real-time Distributed Computing, 2008, pp. 76-82.

[12]. C. Vincent, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, and K. Scarfone, “Guide to Attribute Based Access Control (ABAC) Definition and Considerations,” National Institute of Standards and Technology (NIST Special Publication 800-162), 2014.

[13].W. She, I.-L. Yen, B. Thuraisingham, and E. Bertino, “Policy-Driven Service Composition with Information Flow Control,” 8th IEEE International Conference on Web Services, 2010, pp. 50-57.

[14].Y. Sinjilawi, M. Al-Nabhan, and E. Abu-Shanab, “Addressing Security and Privacy Issues in Cloud Computing,” Journal of Emerging Technologies in Web Intelligence, 2014, vol. 6, no. 2, pp. 192-199.

[15].M. Atallah, M. Blanton, N. Fazio, and K. Frikken, “Dynamic and Efficient Key Management for Access Hierarchies,” ACM Transactions on Information and System Security, 2009, vol. 12, no. 3.

[16]. “Microsoft Developer Network, Identity and Access Management,” http://msdn.microsoft.com/en-us/library/aa 4800 30 .aspx.

[17]. “Gartner, Predicts 2014: Identity and access management,” http://www.gartner.com/.

[18]. N. Li, Q. Wang, W. Qardaji, E. Bertino, P. Rao, J. Lobo, and D. Lin, “Access control policy combining: theory meets practice,” 14th ACM Symposium on Access Control Models and Technologies, 2009, pp. 135–144.

[19]. A. Karp, H. Haury, and M. Davis, “From ABAC to ZBAC: The Evolution of Access Control Models,” HP Laboratories, HPL-2009-30.

[20]. K. C. Feeney, S. N. Foley, and R. Brennan, “A Trust Model for Capability Delegation in Federated Policy Systems,” 6th International Conference on Risk and Security of Internet and Systems, 2011, pp. 1–8.

[21]. P. Mazzoleni, B. Crispo, S. Sivasubramanian, and E. Bertino, “XACML Policy Integration Algorithms,” ACM Transactions on Information System Security, 2008, pp. 852-869.

[22].RFC 2904, “AAA Authorization Framework,” http:// tools.ietf.org/html/rfc2904.

[23].S. Hasani, and N. Modiri, “Criteria Specifications for the Comparison and Evaluation of Access Control Models,” International Journal of Computer Network and Information Security (IJCNIS), 2013, vol.5, no.5, pp. 19-29.

[24]. “Monte Carlo method,” https://en.wikipedia. Org/wiki/ Monte_Carlo_method/.

[25]. M. Casassa Mont, A. Baldwin, and S. Shiu, “Identity Analytics - User Provisioning, Case Study: Using Modelling and Simulation for Policy Decision Support,” HP Laboratories, HPL-2009-57.