International Journal of Industrial Engineering and Management (IJIEM), Vol. 7 No 3, 2016, pp. 111-116
Available online at www.iim.ftn.uns.ac.rs/ijiem_journal.php
ISSN 2217-2661

**UDK: 004.41**

# Applications of Access Control as a Service for Software Security

**Predrag Dašić**
High Technical Mechanical School of Professional Studies, Trstenik 37240, Serbia
SaTCIP Publisher Ltd. Vrnjačka Banja 36210, Serbia, dasicp58@gmail.com
**Jovan Dašić**
SaTCIP Publisher Ltd. Vrnjačka Banja 36210, Serbia
**Bojan Crvenković**
SaTCIP Publisher Ltd. Vrnjačka Banja 36210, Serbia

Received (27.05.2015.); Revised (18.11.2015.); Accepted (09.06.2016.)

**Abstract**

*Cloud technology has been around for some time now and is gaining increased influence in almost every aspect of information technology services. As a consequence of above stated, cloud technology offers improvements to traditional security systems by converging logical (cloud network) and physical security (on-site devices). In this paper, we will discuss the application of Access Control as a Service (ACaaS) for software security systems. ACaaS defines a common policy format for security, the translation of the policy into deployment environments and represents an efficient, cost-effective mechanism for access control.*

**Key words:** *Access Control as a Service (ACaaS); Cloud computing; Cloud security; Security as a Service (SECaaS); Software as a Service (SaaS).*

## 1. INTRODUCTION

Access Control as a Service (ACaaS) offers centralized hosted security solution which integrates cloud computing features on top of existing physical security layer. Such a system for access control brings economic benefits by using a common computing infrastructure for large user groups. Although access equipment needs to be provisioned and installed on-site, the entire process of logical operations is executed in the cloud. This relieves the client from buying and maintaining expensive software and hardware of supportive technology, clients only pay for what he uses.

Most associations keep up numerous, different physical and IT security frameworks with no integration between them. This circumstance has turned into an increasing risk because of security concerns and the need to address protection and administrative consistency. It also helps associations to understand a variety of cost, control, and responsiveness benefits.

ACaaS is required to be developed in a way that it offers compatibility with well-known programming languages and runtime environments along with the support for international standards such as OpenID, OAuth, WS-Trust etc. In addition, ACaaS must be compatible with most of the modern web platforms such as Python, Java, NET, Ruby and PHP. Some real-time implementations of ACaaS are also available in the market; Azure Platform AppFabric Access Control Service, Junos Pulse Access Control Service etc.

An ACaaS comprises of Policy Decision Point (PDP), Policy Enforcement Point (PEP), Policy Administrator Point (PAP) and Policy Information Point (PIP) components. Each of these components can be developed and managed either by the service consumer or they may use the ones provided by the ACaaS provider (trusted third party). To be precise, the access control service provider ensures the segregation and confidentiality of the data contents, even if it gets together with Cloud service consumers and Cloud service providers.

## 2. ACCESS CONTROL AS A SERVICE (ACAAS)

Foundation of ACaaS software is to enable the data separation, concurrency, and manageability that are needed to deliver on the SaaS platform for multiple “tenants” using the same infrastructure at the same time. The primary innovation of ACaaS is that there is no need for dedicated PC or a server at each client’s location for device control. Access is managed through centralized web service as well as other functions like notifications, alarms and reporting.

Communication between users, access devices and web service is done over secure channels using encryption algorithms. These include Internet, cellular, LAN or even satellite connections, depending on the type of security system. System administrators can perform all security management functions from any Internet browser that supports secure connections.

The functions include:

- View event/alarm history
- View stored or live video
- Lock down facility
- Add/delete Credentials
- Add/delete/modify Users, Administrators
- Add/delete/modify Doors/Readers/Elevators/Sensors
- Create/edit email notification rules
- Create/edit schedules
- View permanent journal of administrative actions
- Create and run reports

On Fig. 1 is given a general framework of ACaaS framework proposed by Wu et al. 2016 [1] for public Infrastructure as a Service (IaaS) cloud. The architecture is flexible enough to support role-based access control (RBAC) policies and other security modules. ACaaS module configures RBAC policies and translates them to AWS IAM policies, meaning that the users send access requests to AWS which are controlled by a specific set security policies.

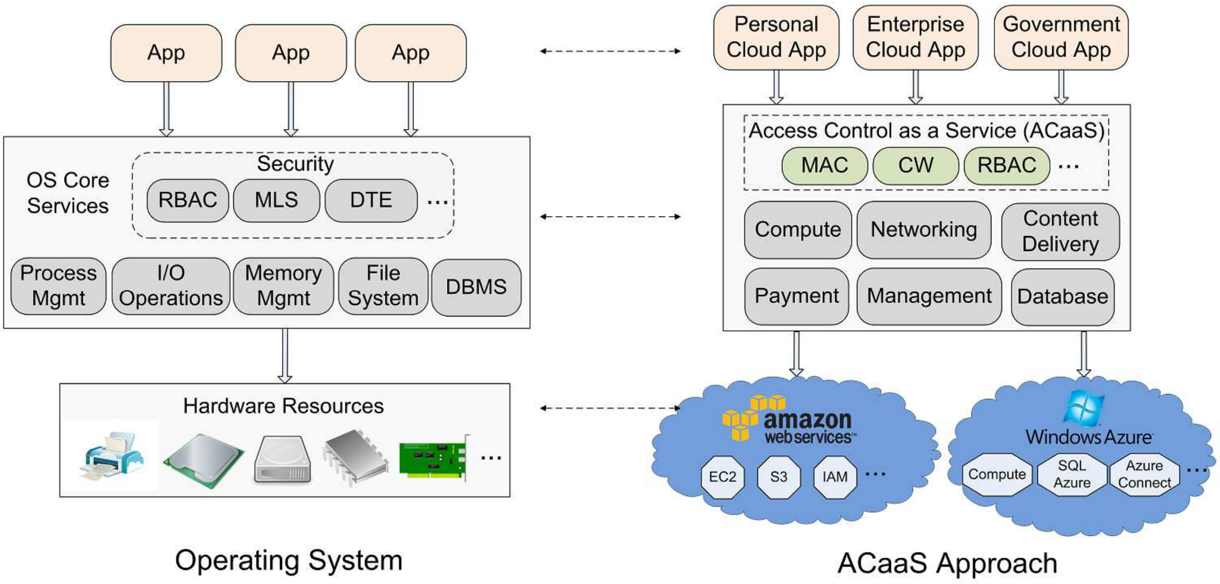

**Figure 1.** ACaaS framework (Wu et al., 2013)

Within ACaaS operate a wide variety of security modules like access management, data encryption, identity federation, identity management, intrusion detection and email security. It can be applied to SaaS, PaaS or IaaS layers to protect the data, applications, as well as the underlying operating system and virtual environment. Although cloud computing is being used for quite some time now, there are still some basic security issues which need to be improved. There are several most fundamental security issues which can be combated by implementing ACaaS as a security layer:

Confidentiality

Khan & Shaheen 2014 [2] propose using randomisation, column-row shuffling and size alteration of matrices for secure cloud transactions to ensure confidentiality of their data without using any additional overhead computation. Their approach suggests that users hold the entire secret values, without sharing with or depending on other parties for a secret key generation, sharing and storing.

Data Integrity

Senthil Kumari, & Nadira Banu Kamal 2016 [3] propose a policy for improving data integrity in the cloud called Key Derivation Policy (KDP). The key generation process includes the data attributes from the combination of local keys by a hash function supported by MAC verification. Decryption is executed with the Cipher Text–Attribute-Based Encryption (CP-ABE) schemes.

Data Location

Fatema, et al. 2015 [4] developed a data location control model which can be applied to ACaaS service. The model translates authorization decisions based on users location into eXtensible Access Control Markup Language (XACML) policies for each data transfer operation. It also provides the users with the information about current data location and any location changes.

Virtualization

Virtualization is a basic component of any cloud infrastructure and is susceptible to security risks mostly from vulnerabilities of VM software. ACaaS is a necessary supporting service and can prevent attackers from obtaining host privileges, execute remote code and modify and control the VM. Win, et al. 2014 [5] proposed a virtualization security solution that combines mandatory access control and virtual machine introspection.

Access control category focuses on account and service hijacking issue which includes fraud, phishing, and other attacks to steal the sensitive credentials of Cloud consumers. Malicious insiders, unreliable authentication mechanisms, privileged user□s access and browser security have been identified as the major issues of this category. Insecure interfaces of APIs are the most focused challenging issues under Cloud infrastructure category which cover various vulnerabilities in a set of APIs provided by cloud providers to their consumers to access services. The quality of service, sharing technical flaws, reliability of suppliers, security misconfiguration, multi-tenancy, server location and backup are the other major security issues in Cloud infrastructure category. Furthermore, Data redundancy, data loss and leakage, data location, data recovery, data privacy, data protection and data availability have been identified as key issues in different scenarios where data has to be properly encrypted, transmitted, secured, controlled and available in the time of need.

## 3. APPLICATIONS OF ACAAS IN SOFTWARE SECURITY

In modern literature, a considerable amount of proposed cloud-based access control mechanisms can be found. Wang et al. proposed an adaptive access control algorithm for cloud computing environments based on the contextual information such as security information and time [6]. In this scheme, authors combined the trust relationship (either between a number of cloud service providers or a cloud service provider) and its consumers with the role-based access control system.

The trust level is updated and changed automatically by the trust management system according to evolution done by clouds after each transaction. In this scheme, authors assume every cloud has a global certificate Authority Authorization Centre (AAC), which is responsible for access control.

Tianyi et al. 2011 [7] proposed the cloud optimized RBAC model (coRBAC). It inherits many features from RBAC and distributed RBAC (dRBAC) such as dRBAC's domain. It merges the dRBAC's distributed authentication services together and gives the CA ability to issue certificates. It also allocates domains for enterprises and companies with the capability to manage their roles and users in their own inner network.

Sun et al. 2012 [8] proposed a semantic access control scheme for cloud computing to authenticate users of health care systems based on ontologies. This scheme implements an access control system in semantic web environments and uses ontologies for the RBAC security model.

The authors extended the RBAC model by using semantic web technologies and utilized the semantic scopes of subjects, objects, actions and attributes to define the relations used in ontologies.

Task-Role-Based Access Control scheme is another access control approach which has been proposed for health care systems in the cloud computing environment [9]. Permissions in Task-Based Authorization Control (TBAC) are activated or deactivated according to the current task or process state. As there is no separation between roles and tasks, they use different factors such as users, information resources, roles, tasks, workflow, and business rules, to solve the separation problem and determine the access control mechanism. The scheme uses the workflow authorization model for synchronizing workflow with authorization flow.

A reference ontology framework using Role-Based Access Control model was proposed by Tsai and Shao 2011 [10]. It aims at providing an appropriate policy with an exact role for every tenant. In this approach, a subject can have multiple roles in different sessions. In addition, a role hierarchy is based on domain ontology and can be transferred between various ontology domains.

Different policies are used to grant permissions such as access policy and security policy. Policies might be used as components of a role according to the role's characteristics, such as a priority and business values.

Mon & Naing 2011 [11] proposed a privacy enhancement system on academic-based private cloud system using Eucalyptus open source cloud infrastructure, and they call it Attribute Role Based Access Control (ARBAC). Their solution tries to guarantee the privacy of cloud's users and security of the personal data, by combining two approaches together, which are role-based access control and attribute-based access control model.

Authors Younis, et al. 2014 [12] proposed a model Access Control model for Cloud Computing (AC3) that facilitates the role and task principles to meet the identified cloud access control requirements. In the model, users are classified according to their actual jobs. Thus, users will be located on a security domain that relates to their role. Every role within the model will be assigned a set of the most relevant and needed tasks for practicing this role.

Every task will have a security classification for accessing the data or assets, and the exact permissions needed for accomplishing this task. A risk engine is utilized to deal with dynamic and random behaviors of users; it credits consumers according to their access behaviors.

Amazon AWS Identity and Access Management (IAM) [14] is the integration of an identity management system and an access control mechanism. Upon subscribing to an Amazon AWS product, each customer is assigned an AWS tenant account. All operations on AWS products are then bound to this account. Amazon IAM provides a mechanism to create and manage multiple users binding to the AWS tenant account.

Using JSON-style authorization policies storing at the IAM side or attaching at the AWS product side, the IAM could control user activities on AWS resources. To guarantee security requirements on confidentiality and integrity, users are allocated their own security credentials to access AWS resources. On Fig. 2 is shown the flow diagram of Amazon's Identity and Access Management.

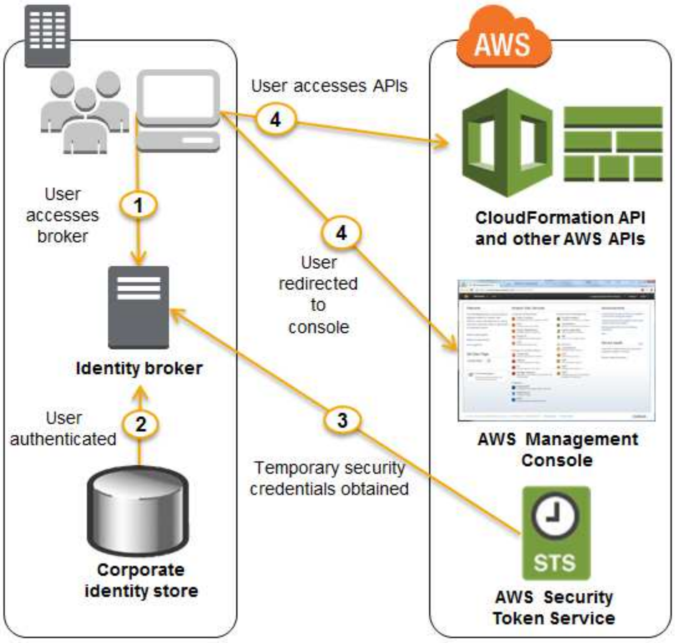
AWS
User accesses APIs
4
CloudFormation API and other AWS APIs
User accesses broker
1
4
User redirected to console
Identity broker
AWS Management Console
User authenticated
2
3
Temporary security credentials obtained
STS
Corporate identity store
AWS Security Token Service

**Figure 2.** Flow diagram of Amazon's Identity and Access Management. Source: (Amazon)

Based on the Common Information Model (CIM), authors Bernabe et al. 2012 [15] and Calero et al. 2010 [16] proposed a RBAC model integrating with the CIM. In this work, an authorization statement defined as the 4-tuple of the issuer, subject, privilege, resource is written as a rule using Semantic Web Rule Language (SWRL) [17]. The rule is then reasoned by a DL Reasoner to transform into RDF statements. Authors illustrated that it is possible to use proposed model to support RBAC features for users of a tenant. Inter-tenant collaborations are represented by sharing context information, so the trustee can define authorization statements.

The Multi-tenant Role-based Access Control (MT-RBAC) [18] extended the basic RBAC with a set of models including administration features. Beside regular intra-tenant permission and role assignment operations, the cross-tenant collaborations are performed by sharing roles. The truster tenant can define either all roles to trustee tenants, the same public roles to all trustees, or separated public roles to different trustees. In turn, the trustee can perform two administrative operations: user assignment (UA) to its users and role hierarchy on the shared roles.

Jin et al. 2014 [19] extended the ABAC model from previously developed [20] to IaaS scenarios. In their model, entities were classified into cloud root user who can manage Virtual Infrastructure (VI) and tenants; tenant root user who can configure attribute profile and manage tenant admin users; tenant admin users in a tenant can manage tenant regular users and finally tenant regular users who can operate on cloud resources.

To protect data in outsourced environments like clouds, ABE research [21-23] was proposed for the security of outsourcing storage, while homomorphic encryption [24,25] was proposed to secure computation on hostile systems. In the key-policy ABE approach (KP-ABE) [22], request attributes were associated to ciphertexts, and policies were associated with users' keys. The ciphertext-policy ABE (CP-ABE) scheme Bethencourt et al., 2007 provided a mechanism that allows creating users' keys based on their attributes, and attribute-based policies to protect data are associated in ciphertexts. The ABE schemes were extended and applied to secure data on cloud storage services [26]. Although the homomorphic encryption may provide confidentiality in outsourcing computation, its applications on cloud were still limited due to the complexity and performance overhead (Naehrig et al., 2011).

OAuth authorization framework [27] enables a third-party to access an HTTP resource by approval of the data owner via tokens. It provides a workflow protocol for distributed authorization currently applied in various cloud-based services such as Google APIs and Twitter APIs. However, OAuth 2.0 does not use any cryptographic mechanism but relies its security based on HTTPS, which is not flexible in scenarios when clients using proxies or cannot have direct connections with the resources.

In a paper by Ngo, et al. 2016 [13] authors presented a multi-tenant attribute-based access control (MT-ABAC) model for cloud services in which the access control model is integrated with the cloud infrastructure information description model. Their approach not only can generate provider delegation policy automatically from cloud resource descriptions but also can support multiple levels of delegations with high flexibility for inter-tenant collaborations. They also extended the MT-ABAC for distributed, multiple collaborative cloud providers in the hierarchy to support Intercloud scenarios with exchanging tokens approach.

Access control is an integral part in cloud environment used in majority of service models such as Search as a Service (SaaS) [28,29], where access is managed for search privileges (public-private indices), and results representation and Video Surveillance as a Service (VSaaS) [30,31] where access control is of utmost importance for managing recorded media. An example of access managed search are scientific databases Scopus-Elsevier and WoS-Thomson Reuters.

Google's Cloud IAM functions on same principles as AWS and can manage access privileges to Google account, service account, Google group, Google for work domain. Fig 3. illustrates Google's IAM workflow.

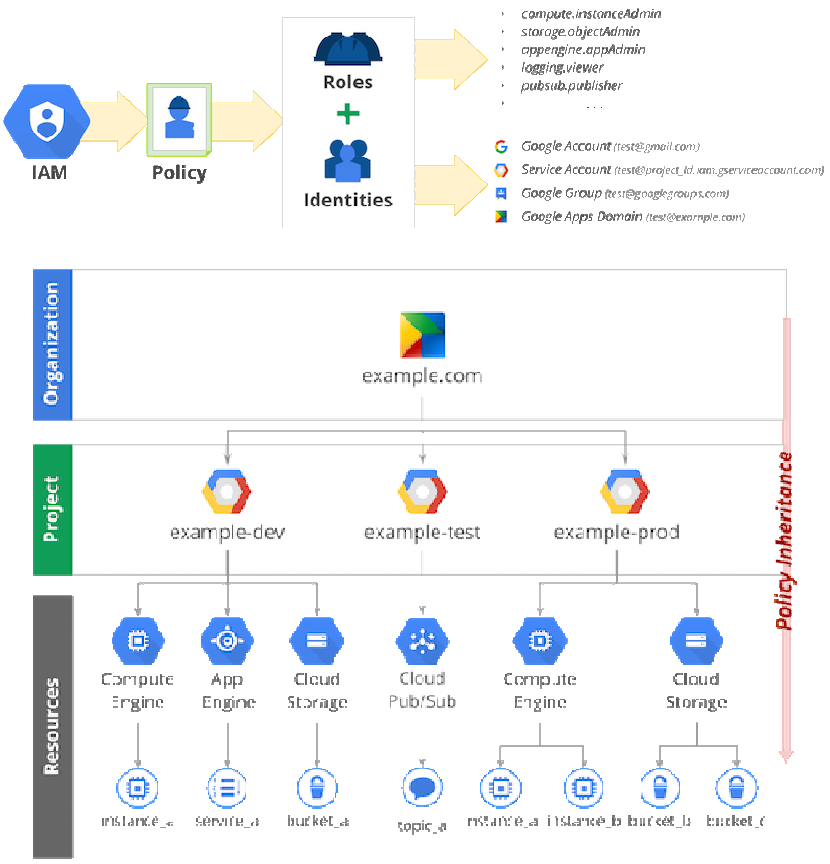

**Figure 3.** Google's IAM workflow

## 5. CONCLUSION

Cloud computing offers services for consumers through effective utilization of shared resources. Despite its effectiveness for cloud service providers as well as for the cloud users, its prevalence is hindered by various security issues. This paper presents a comprehensive survey of the issues and research contributions for cloud-based access control. Surveyed literature shows rapid development in this field with a considerable amount of new model proposals and as well improvements on existing models. Maintaining security of software and devices is of imperative importance in a business environment. ACaaS reduces overall costs and offers unsurpassed technological possibilities compared to traditional systems which should be fully utilized.

## 6. REFERENCES

[1] Wu, R., Zhang, X., Ahn, G.-J., Sharifi, H. and Xie, H. (2013), *"ACaaS: Access control as a service for IaaS cloud"*, In Proceedings - SocialCom/ PASSAT/ BigData/ EconCom/ BioMedCom, pp. 423-428.

[2] Khan, K.M. and Shaheen, M. (2014), *"Empowering users of cloud computing on data confidentiality"*, in 3rd International Conference on Cloud Networking (CloudNet) in Luxembourg, IEEE, Piscataway, pp. 272-274.

[3] Senthil, K.P., Banu, N. and Kamal, A.R. (2016), *"Key derivation policy for data security and data integrity in cloud computing"*, Automatic Control and Computer Sciences, Vol. 50, pp. 165-178.

[4] Fatema, K., Healy, P.D., Emeakaroha, V.C., Morrison, J.P. and Lynn, T. (2015), *"A data location control model for cloud service deployments cloud computing and services sciences"*, in International Conference in Cloud Computing and Services Sciences (CLOSER-2014) in Barcelona, Spain, Springer International Publishing, Berlin-Heidelberg, pp. 117-133.

[5] Win, T.Y., Tianfield, H. and Mair, Q. (2014), *"Virtualization security combining mandatory access control and virtual machine introspection"*, in 7th International Conference on Utility and Cloud Computing (UCC-2014), IEEE/ACM, London, pp. 1004-1009.

[6] 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 6th International Conference on Pervasive Computing and Applications, IEEE, Piscataway, Article no. 330e4.

[7] 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, IEEE, Piscataway, Article no. 97e102.

[8] Sun, L., Wang, H., Yong, J. and Wu, G. (2012), *"Semantic access control for cloud computing based on e-Healthcare"*, in Proceedings of the 16th International Conference on Computer

Supported Cooperative Work in Design (CSCWD-2016), IEEE, Piscataway, Article no. 512e8.

[9] Andal, J.H. and Hadi, G.M. (2011), *"Ensuring access control in cloud provisioned healthcare systems",* in Consumer Communications and Networking Conference (CCNC-2011), IEEE, Piscataway, Article no. 247e51.

[10] Tsai, W.-T. and Shao, Q. (2011), *"Role-based access-control using reference ontology in clouds",* in 10th International Symposium on Autonomous Decentralized Systems, Vol. 2, IEEE, Piscataway, Article no. 121e8.

[11] Mon, E.E. and Naing, T.T. (2011), *"The privacy-aware access control system using attribute-and role-based access control in private cloud",* in 4th International Conference on Broadband Network and Multimedia Technology, IEEE, Piscataway, Article no. 447e51.

[12] Younis, A.Y., Kifayat, K. and Merabti M. (2014). "*An access control model for cloud computing*", Journal of Information Security and Applications, Vol. 19, pp. 45-60.

[13] Ngo, C., Demchenko, Y. and de Laat, C., (2016), *"Multi-tenant attribute-based access control for cloud infrastructure services",* Journal of Information Security and Applications, Vol. 27-28, pp. 65-84.

[14] Amazon. AWS Identity and Access Management (IAM), <http://aws.amazon.com/iam/>; (Accessed: 15 October 2016).

[15] Bernal, B.J., Marin, P.J.M., Alcaraz, C.J.M., Garcia, C.F.J., Martinez, P.G. and Gomez, S.A.F. (2012), *"Semantic-aware multi-tenancy authorization system for cloud architectures",* Future Gener Comput Syst, Vol. 32, pp.154-67.

[16] Calero, J.M.A., Edwards, N., Kirschnick J., Wilcock, L. and Wray, M. (2010), *"Toward a multi-tenancy authorization system for cloud services",* IEEE Secur Priv, Vol. 8, pp. 48–55.

[17] Horrocks, I., Patel-Schneider, P.F., Boley, H., Tabet, S., Grosof, B. and Dean, M. *"SWRL: A semantic web rule language combining OWL and RuleML",* W3C Member Submission World Wide Web Consortium. <http://www.w3.org/Submission/SWRL/

[18] Tang, B., Li, Q. and Sandhu, R.A. (2013), *"Multi-tenant RBAC model for collaborative cloud services",* in 11th Annual International Conference on Privacy, Security and Trust (PST), IEEE, Piscataway, pp. 229-238.

[19] Jin, X., Krishnan, R. and Sandhu, R. (2014), *"Role and attribute based collaborative administration of intra-tenant cloud IAAS",* in International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), IEEE, Piscataway, pp. 261-274.

[20] Jin, X., Krishnan, R. and Sandhu, R. (2012), "*A unified attribute-based access control model covering DAC, MAC and RBAC*", Lecture Notes in Computer Science, Vol. 7371, pp. 41-55.

[21] Bethencourt, J., Sahai, A. and Waters, B. (2007), *"Ciphertext-policy attribute based encryption",* in Symposium on Security and Privacy (SP'07), IEEE, Piscataway, pp. 321-334.

[22] Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006), *"Attribute-based encryption for fine-grained access control of encrypted data",* in Proceedings of the 13th Conference on Computer and Communications Security, ACM, New York, pp. 89-98.

[23] Sahai, A. and Waters, B. (2005), *"Fuzzy identity-based encryption",* in Advances in Cryptology - EUROCRYPT-2005, Springer, Berlin-Heidelberg, pp. 457-73.

[24] Brakerski, Z. and Vaikuntanathan, V. (2011), *"Efficient fully homomorphic encryption from (standard) lwe",* in 52nd Annual Symposium on Foundations of Computer Science (FOCS-2011), IEEE, Piscataway, pp. 97-106.

[25] Smart, N.P. and Vercauteren, F. (2010), *"Fully homomorphic encryption with relatively small key and ciphertext sizes",* in Public Key Cryptography (PKC-2010). Springer, Berlin-Heidelberg,, pp. 420-443.

[26] Li, M., Yu, S., Zheng, Y., Ren, K. and Lou, W. (2013), *"Scalable and secure sharing of personal health records in cloud computing using attributebased encryption",* IEEE Trans Parallel Distrib Syst, Vol. 24, pp.131-143.

[27] Hardt, E. and Recordon, D. (2016) The OAuth 2.0 Authorization Framework, draft-ietf-oauth-v2-30. Technical Report. <http://tools.ietf.org/ html/draft-ietf-oauth-v2>; (Accessed: 15 October 2016)

[28] Dašić, P., Dašić, J. and Crvenković, B. (2016), "*Service models for cloud computing: Search as a service (SaaS)*", International Journal of Engineering and Technology, Vol. 8, Issue 5, pp. 2366-2373.

[29] Dašić, P., Dašić, J. and Crvenković, B. (2016), *"Applications of the Search as a Service (SaaS)"*, Bulletin of the Transilvania University of Braşov, Series I: Engineering Sciences, Vol. 9, No. 2, pp. 91-98

[30] Dašić, P., Dašić, J. and Crvenković, B. (2016), "*Service models for cloud computing: Video Surveillance as a Service (VSaaS)"*, Bulletin of the Transilvania University of Braşov, Series I: Engineering Sciences, Vol. 9, No. 2, pp. 83-90.

[31] Dašić, P., Dašić, J. and Crvenković, B. (2016) "*Some examples of Video Surveillance as a Service applications*", in Proceedings of the 7th International Multidisciplinary Scientific Symposium "Sustainable Development Through Quality and Innovation in Engineering and Research" (SIMPRO-2016), University of Petroşani, Petroşani, Romania, pp. 367-370.

# Primene kontrole pristupa kao servis za softversku sigurnost

**Predrag Dašić, Jovan Dašić, Bojan Crvenković**

Primljen (27.05.2015.); Recenziran (18.11.2015.); Prihvaćen (09.06.2016.)

## Abstrakt

*Cloud tehnologija je prisutna već neko vreme i postiže značajan uticaj na skoro svaki aspekt usluga u informacionoj tehnologiji. Kao posledica gore navedenog, cloud tehnologija nudi poboljšanja tradicionalnim sigurnosnim sistemima konvergencijom logičkog (cloud mreža) i fizičkog obezbeđenja (uređaji na licu mesta). U ovom radu je data diskusija o primeni kontrole pristupa kao servisa (eng. Access Control as a Service - ACaaS) za softverske sigurnosne sisteme. ACaaS definiše zajednički format polise za sigurnost, prevođenje polise u izvršna okruženja i predstavlja efikasan i pristupačan mehanizam za kontrolu pristupa.*

**Key words:** *Kontrola pristupa kao servis (ACaaS); Klaud računarstvo; Klaud sigurnost; Sigurnost kao servis (SECaaS); Softver kao servis (SaaS).*