Analyzing Recent Trends in Enterprise Identity Management

Michael Kunz, Matthias Hummer, Ludwig Fuchs, Michael Netter and Günther Pernul
Department of Information Systems
University of Regensburg
Regensburg, Germany
{firstname.lastname}@wiwi.uni-regensburg.de

***Abstract*—Recent data breaches caused by highly-privileged insiders (e.g. the NSA/Snowden case) as well as the proliferation of mobile and cloud applications in enterprises imposes new challenges for Identity Management. To cope with these challenges, business analysts have predicted a variety of trends for enterprise Identity Management. In this paper, we conduct a thorough literature analysis to examine to which extent the scientific community seizes upon these trends and identify major research areas therein. Results show that despite the analysts' predictions, research stagnates for attribute-based access control and privileged user management, while for cloud-based IdM and bring your own device it corresponds to the analysts' forecast.**

I. Introduction

Effectively administrating employees' access to sensitive applications and data is a central challenge for today's organizations. A typical large organization manages millions of user access privileges spread across thousands of IT resources. Recent governance and compliance mandates have amplified the importance of establishing an enterprise-wide Identity Management infrastructure. Traditionally, IdM has been associated with storing user data, maintaining user accounts, and controlling users' access to applications. Within that area, research has provided adequate measures throughout the last decades for securing user and entitlement management. At the same time, a market for solutions applying those concepts has developed providing basic IdM-functionalities like automated user (de-) provisioning, role-based access control (RBAC), or workflow capabilities for realizing a business-driven allocation of access privileges. In the recent past, however, a convergence and integration of new technologies for improving enterprise IdM can be recognized. Developments concerning the fields of cloud computing, mobile computing, federated identity structures among organizations, or flexible context-based assignment of access privileges more and more are seen as a part of enterprise IdM. As a result, a vivid practical as well as a research community dealing with these emerging issues has evolved.

Following a structured research approach, this paper aims at investigating the currently prevalent trends in enterprise IdM predicted by analyst firms and examines to which extent the scientific community seizes upon these predictions. In order to achieve that goal we initially inspected a broad spectrum of widely recognized reports recently published by the following analyst firms: Capgemini [1], Ernst & Young [2], Gartner [3], Forrester [4], and KuppingerCole [5], [6].

An in-depth analysis of those reports revealed four major trends in enterprise IdM: The application of *attribute-based access control (ABAC)*, the integration of the emerging *bring your own device (BYOD)* concept, *cloud-based Identity Management*, and *privileged user management*. A thorough literature analysis of research output for each of these four trends needs to be conducted in order to highlight and evaluate research activities and main areas of focus of scientific publications. Note that additional minor tendencies, e.g. dealing with the extension of already available IdM-functionality or organizational issues during IdM-adoption within enterprises can be found. Due to the focus of this paper on the major trends, they are not considered in the remainder.

The remainder of this paper is structured as follows: in the next section, the research methodology is presented. Subsequently, we assess the extent to which the scientific community seizes upon the analysts' predictions and trends and highlight main areas of research. Section IV concludes the paper, outlining implications and areas for future work.

II. Research Methodology

Our research follows the methodology shown in Figure 1. Based on predictions of recognized analysts (step 1), we identify major trends and topics, which are discussed in Section III-A.

In a second step, those major trends serve as input for a literature analysis following the methodology proposed in [7]. To arrive at a broad coverage of scientific publications, the following literature databases were selected: DBLP[1], the ACM Digital Library[2], the IEEE Digital Library[3], and Google Scholar[4]. We employed a systematic keyword-based search technique to arrive at a comprehensive set of relevant literature. To generate appropriate search terms, each previously identified trend (and its abbreviations) are used as keywords complemented by the term "identity management". To identify recent trends in scientific literature, we limited the search period to the last four years (2010 - 2013).

[1] http://www.dblp.org/search/index.php
[2] http://dl.acm.org/
[3] http://www.computer.org/
[4] http://scholar.google.com/

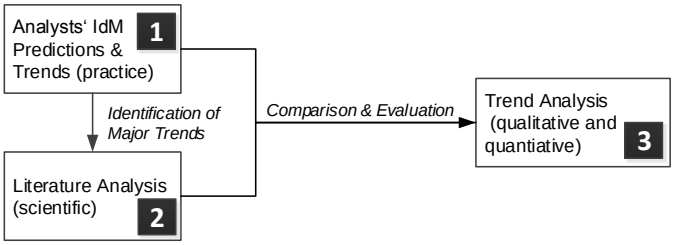

Fig. 1. Research methodology

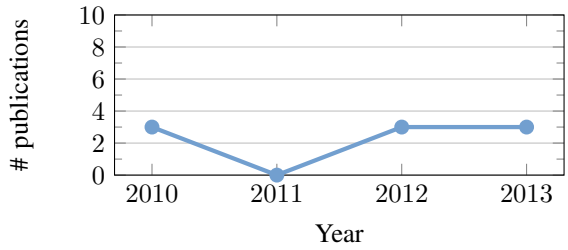

Fig. 2. Publications dealing with privileged user management per year

Lastly, results from the literature analysis were compared with the analysts' forecast (step 3). In particular, we quantitatively evaluate for each trend whether the growth rate of scientific publications matches the predictions. Additionally, we identify trending research areas and qualitatively discuss deviations from the predicted trend.

III. Trends in Enterprise Identity Management

We up to now have shown that four major trends for the future of enterprise IdM have been predicted by analysts. Following our research methodology (cf. Section II), we firstly provide a definition for each of the four trends and discuss the analysts' viewpoint (Section III-A). Subsequently, the scientific research activities for each trend are evaluated in detail. Initially, we quantitatively analyze the growth rates of publications. On a qualitative level, we identify the main areas of research for each trend and summarize representative publications. Note that our goal is to highlight existing research directions for each of the predicted trends. We are aware that besides the presented research, several other popular research directions including identity federation management or risk and trust management within the field of enterprise IdM exist.

A. Definition of trends

Prior to a detailed evaluation, the goal of this section is to provide a definition for each trend in order to gain a common understanding and discuss the analysts' reasons to name it an emerging field for future enterprise IdM.

a) ***Privileged User Management****:* refers to processes, policies, and technologies that aim to control, limit, and audit accounts with elevated privileges (such as system administrators). While it has long been a key challenge for IdM in organizations, insider threats such as the NSA/Snowden security breach bring privileged user management into the limelight again and put it on analysts' agendas. Furthermore, coping with privileged users and setting up general guidelines as well as introducing technical measures become mandatory tasks due to emerging regulatory or certification requirements.

b) ***ABAC****:* constitutes an access control scheme where authorizations are assigned based on attributes associated with the requesting subject, the requested operations and resources, and additional environmental properties (such as time and the requester's location) [8]. According to Gartner [3], 70 % of all businesses will use ABAC to protect critical assets by 2020. In contrast to newly emerging fields that are based on recent developments (like cloud-based IdM or BYOD), ABAC roots in the area of access control tracing back several decades.

c) ***BYOD****:* refers to an emerging desire of employees to bring their own mobile devices into the workplace to access corporate data. Rather than being able to use well-defined security measures such as firewalls or appropriately configured devices to prevent unauthorized access and data leakage [9], BYOD requires new approaches to IT security in general and innovative IdM concepts in particular. Analysts' predictions include improved authentication mechanisms tailored for mobile usage [4], user-friendly interfaces to access data, and flexible policies to manage access.

d) ***Cloud-based IdM****:* comprises the shift from on-premise IdM solutions to outsourcing identities (Identity as a service, IDaaS), applications, and systems to the cloud. Furthermore, cloud-based IdM deals with the management of on-premise IdM-architectures connected to cloud-based services. Benefits of cloud-based IdM stated by analysts include reduced cost of ownership, reduced deployment time and minimizing the overhead of managing related IT infrastructure. At the same time, challenges that emerge when adopting a cloud-based IdM strategy need to be resolved. These span areas from securely managing access to the data and privacy issues to trust requirements related to the cloud service provider.

B. Privileged User Management

Despite being highlighted as a future trend in IdM by analysts only little research has been conducted in the field of privileged user management during the last years (see Figure 2). The publication count indicates a low level of general research activities with about two publications per year. Several of them appeared as practical reports (e.g. [10] or [11]), further underlining the topic's practical relevance. However, only little theoretical research work can be found in the area over the last years. One explanation for this fact might be that the management of privileged accounts is not a new research challenge but rather has been dealt with since the advent of access control models. Newly established compliance mandates and the emerging need for controlled IdM processes due to financial scandals and various insider abuse incidents, however, have led to an increased practical interest in solutions (technical as well as organizational) to tackle the challenge.

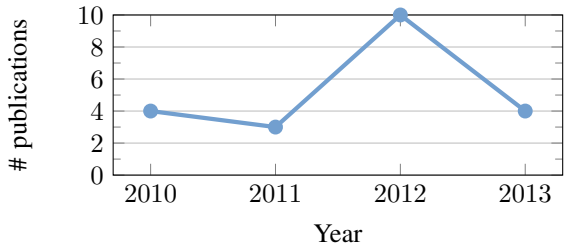

Fig. 3. Publications dealing with ABAC per year

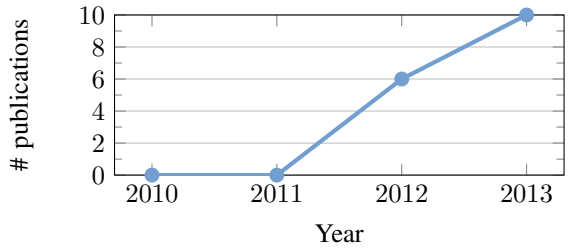

Fig. 4. Publications dealing with BYOD per year

Reviewing existing research work prior to the year 2010 reveals several administrative models for access control models that deal with the issue of managing administrative users and access control models in general. Recent surveys, for instance, underline the amount of research being conducted in the area of administrating RBAC as the most widely used access control model in enterprise IdM scenarios [12].

Regarding research directions in the area, several trends can be observed. On the one hand, researchers deal with the issue of privileged user management in cloud environments (e.g. [13]). On the other hand, authors like [11] investigate general issues like auditing challenges, shared accounts, or log file manipulation by superusers. Besides, conceptual solutions that aim at automating privileged user management including provisioning and auditing processes have been proposed [14]. However, due to the relatively small amount of research work, those tendencies cannot be considered stand-alone research areas. In general, privileged user management seems to remain a rather practical issue amplified by the emerging trend of IT governance, compliance, and risk management in the field of IdM. An increased importance of the topic among researchers within the next years is not expected.

C. Attribute-based Access Control (ABAC)

Figure 3 displays the recent evolution of publication counts related to ABAC in the context of enterprise IdM. The number of publications per year varies, yet, in contrast to the analysts' prediction of a generally growing importance of ABAC, neither an uptrend nor a downtrend can be identified in the resarch community. The lack of increase in scientific publications may stem from the already achieved maturity of ABAC research in general due to its roots in the area of access control mechanisms tracing back several decades. Qualitatively assessing ABAC-related publications reveals three major areas of research, which are subsequently discussed.

1) Implementation models and architectures: Firstly, ABAC models and architectures are developed due to the evolving landscape in which IdM systems reside. This evolution includes the shift towards cloud computing, the increasing number of devices connected to enterprise IdM systems, and the rising number of attributes allowing for authorizations to be assigned based on the current context. In [15], for instance, privileges for collaborative environments are granted and revoked dynamically based on the historical behavior of a user. Besides, in [16] an ABAC-based model for highly dynamic real-time applications such as smart grids, where time constraints imposed by physical processes must be met when deciding upon access requests, is presented.

2) ABAC in cloud computing: Secondly, researchers focus on the role of ABAC to protect corporate information in off-premise cloud-based environments. For example, [17], [18], and [19] present ABAC implementations in cloud collaboration scenarios that aim at overcoming challenges such as the management of globally accessing resources and the scalability of access control mechanisms in the context of an increasing number of devices.

3) Transition from RBAC to ABAC: Thirdly, a significant number of publications deals with the shift from RBAC towards ABAC. Sandhu [20] discusses the benefits and challenges of this transition for enterprise access control. Similarly, results of the comparison of both models in [21] stress both, the simplicity and usability of RBAC, as well the superior flexibility and granularity of ABAC. Besides, a significant body of research focuses on combining both models in order to harness their advantages [22], [23], [24], [25]. They cover aspects such as dynamic role activation based on specific attributes (e.g. the current date) and applying additional constraints to reduce permissions of a role available to the user.

D. Bring your own device (BYOD)

The number of publications dealing with BYOD in the area of enterprise IdM is depicted in Figure 4 with the first publications appearing in the year 2012. Since then, a significant rise of research output in 2013 can be recognized, clearly underlining the increasing importance of BYOD within the research community. The growth rate of academic publications over the last two years corresponds to the analysts' predictions which foresee the impact of the increasing shift to mobile computing on enterprise IdM. A detailed assessment of recent BYOD-related research activities in detail, reveals the following two major areas.

1) Identification of current challenges: Morrow provides an overview of current security challenges that emerge due to the increasing adoption of BYOD [26]. These include viruses and other malware threats existing on unmanaged consumer devices that are difficult to control by traditional corporate IT security measures. Underlining this threat, a recent survey

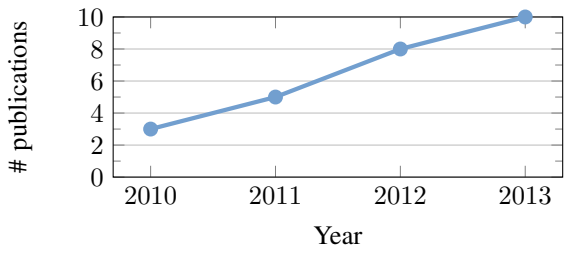

Fig. 5. Publications dealing with cloud-based IdM per year

of Infonetics Research[5] shows, that nearly all questioned enterprises had malicious applications on at least one of their mobile devices. Besides, the use of cloud technologies on mobile devices imposes a major threat [27]. Erroneously assigned rights to access data on a cloud storage (e.g. by mistake), for instance, may inappropriately release critical corporate data to the public.

2) Conceptual and technical solutions: Approaches to solve the emerging challenges regarding BYOD can be found on different levels of abstraction. On a conceptual level, several researchers argue to establish different trust zones for different types of devices [28], [29]. In order to realize these concepts, technical measures need to be defined. A comprehensive technical architecture on how to realize mobile access on corporate data has, for instance, been proposed in [30]. Besides, the capabilities of mobile devices (such as sensors) offer a variety of new means to authenticate users. [31], for instance, present an approach for combining data from various mobile sensors in order to determine the user's context which is subsequently used for authentication.

E. Cloud-based Identity Management

In recent years, the cloud-computing paradigm has become an emerging topic in information systems and computer science research. IdM is involved in most cloud-based scenarios such as IDaaS applications, research on inter-cloud connectivity, and the presentation of fundamental security mechanisms (authentication, authorization, and access control) in the context of cloud computing. Despite this significant body of cloud-related research, only a small portion of publications explicitly focuses on enterprise IdM. Figure 5 depicts the four-year evolution of the respective publication count, showing a slow, yet steady rise of publications per year. This trend corresponds with the analysts' predictions of enterprises seizing upon cloud-based IdM and the resulting need for research in this area. In particular, we identified the following three main areas of interest for researchers.

1) Security: Security in general has been identified as one of the major obstacles of enterprise cloud adoption [32] and is thus in the focus of IdM-related cloud research. An overview of security requirements for cloud-based IdM is provided in [13]. Similarly, Jana and Bandyopadhyay identify threats in cloud environments and outline best practices to mitigate these risks [27]. Besides, several approaches particularly focus on access control in the cloud [33], [34].

2) Standardization: Theoretical research aims to develop standards and protocols for cloud-based IdM to increase the CIO/CSO's trust in off-premise solutions. A review of existing standards as well as an analysis of the requirements of a cloud provider and cloud user together with an assessment of the maturity level of each standard are provided in [35]. In a similar fashion, Lonea et al. review existing IdM standards regarding their usage in cloud-based environments [13].

3) Risk: An additional area of interest for researchers is the assessment of risks that are associated with the shift from on-premise to off-premise solutions. In [36], for instance, a risk-based assessment of data and its protection requirements is conducted, underlining that cost savings can be achieved without compromising critical data. Besides, [37] focus on the quantification of risks in cloud-based IdM topics (e.g. security, privacy, and interoperability) whereas [38] propose an cloud-based architecture for authentication through risk scores.

IV. Conclusions

Over the last decades, secure enterprise-wide identity management has gained significant importance when dealing with security challenges in medium-sized and large organizations. After the settlement of basic IdM-functionalities and their dissemination in practice, recent trends towards opening up previously closed IdM infrastructures of companies towards the integration of emerging technologies like cloud computing and federated identity structures integrating the users' mobile devices can be noticed. Various analysts recently predicted the adoption of BYOD, cloud computing technologies, flexible ABAC mechanisms, as well as privileged user management. This paper examined the adoption of those trends in the research community. The results underline that, while privileged user management and ABAC concepts are not seen as a new challenge leading to increased research output, BYOD as well as cloud-based IdM have both gained significant attention in the research community.

Cloud computing can be interpreted as a comprehensive research area in which identity-related challenges constitute only one aspect of interest. Researchers on the one hand interpret IdM in cloud computing as providing Identity-as-a-Service for enterprises, essentially outsourcing IdM infrastructures. On the other hand, issues dealing with the creation, usage, and revocation of identities enabling the usage of cloud-based services by employees and users in general are discussed. At the same time, BYOD has become popular in the community throughout the last two years. As IdM is an essential aspect of BYOD, the trend towards an increased research output in that area is not surprising. The rise of mobile devices has impacted the business environment of enterprises for several years now. Increasing flexibility and usability for end users thus requires new concepts to extend existing IdM infrastructures. ABAC, on the contrary is not a new trend within the research community. The concept has been prevalent for several years

[5]http://www.infonetics.com/pr/2012/Enterprise-Mobile-Security-Strategies-Survey-Highlights.asp

and only recently is gaining practical importance. As a result, no significant rise in research output has been noticed throughout the last years. The same holds for privileged user management which can merely be seen as a research trend. Its predicted growing practical importance rather might stem from a generally increasing relevance of compliance with regulatory measures and increased public awareness regarding insider threats often caused by over-privileged employees with administrative permissions.

ACKNOWLEDGMENT

The research leading to these results was supported by the "Bavarian State Ministry of Education, Science and the Arts" as part of the FORSEC research association.

REFERENCES

[1] Capgemini, "Studie IT-Trends 2014," Tech. Rep., 2013. [Online]. Available: http://www.de.capgemini.com/resource-file-access/resource/pdf/capgemini-it-trends-studie-2014.pdf (retrieved on 03/30/2014)

[2] Ernst & Young, "Identity and Access Management - Beyond Compliance," Tech. Rep., 2013. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_and_access_management_Beyond_compliance_AU1638.pdf (retrieved on 03/28/2014)

[3] A. Allan, G. Kreizman, E. Perkins, F. Gaehtgens, and B. Iverson, "The Identity and Access Management Scenario: The Future of Managing Identity," 2013. [Online]. Available: http://events.gartner.com/ja/symposium/eu/symposium/esc25/events agenda/details/714 (retrieved on 03/26/2014)

[4] E. Maler, "Navigate The Future Of Identity And Access Management," Forrester, Tech. Rep., 2012. [Online]. Available: http://www.forrester.com/Navigate+The+Future+Of+Identity+And +Access+Management/fulltext/-/E-RES61625 (retrieved on 03/28/2014)

[5] KuppingerCole, "Privilege Management," Tech. Rep., 2013. [Online]. Available: https://www.kuppingercole.com/report/advisory note_privilegemanagement_707369413 (retrieved on 03/29/2014)

[6] KuppingerCole, "Top Trends 2012-2013," Tech. Rep., 2012. [Online]. Available: http://www.kuppingercole.com/report/trendreport top2012200412 (retrieved on 03/28/2014)

[7] Y. Levy and T. J. Ellis, "A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research," *Informing Science Journal*, vol. 9, pp. 181–212, 2006.

[8] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," *NIST Special Publication*, vol. 800, p. 162, 2014.

[9] T. Brooks, "Classic enterprise IT: the castle approach," *Network Security*, vol. 2013, no. 6, pp. 14–16, 2013.

[10] S. Dinoor, "Privileged Identity Management: Securing the Enterprise," *Network Security*, vol. 2010, no. 12, pp. 4–6, 2010.

[11] J. Grafton, "Avoiding the Five Pitfalls of Privileged Accounts," *Network Security*, vol. 2013, no. 5, pp. 12–14, 2013.

[12] L. Fuchs, G. Pernul, and R. Sandhu, "Roles in Information Security – A Survey and Classification of the Research Area," *Computers & Security*, vol. 30, no. 8, pp. 748 – 769, 2011.

[13] A. Lonea, H. Tianfield, and D. Popescu, "Identity Management for Cloud Computing," in *New Concepts and Applications in Soft Computing*, ser. Studies in Computational Intelligence, V. E. Balas, J. Fodor, and A. R. Varkonyi-Koczy, Eds. Springer, 2013, vol. 417, pp. 175–199.

[14] R. Walters, "The Cloud Challenge: Realising the Benefits Without Increasing Risk," *Computer Fraud & Security*, vol. 2012, no. 8, pp. 5–12, 2012.

[15] H. Ould-Slimane, M. Bande, and H. Boucheneb, "WiseShare: A Collaborative Environment for Knowledge Sharing Hoverned by ABAC Policies," in *CollaborateCom*, 2012, pp. 21–29.

[16] M. Burmester, E. Magkos, and V. Chrissikopoulos, "T-ABAC: An Attribute-Based Access Control Model for Real-Time Availability in Highly Dynamic Systems," in *Proc. of the IEEE Symposium on Computers and Communications (ISCC)*, 2013, pp. 143–148.

[17] Z. Iqbal and J. Noll, "Towards Semantic-Enhanced Attribute-Based Access Control for Cloud Services," in *Proc. of the 11th Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2012, pp. 1223–1230.

[18] F. Liang, H. Guo, S. Yi, and S. Ma, "A Multiple-Policy supported Attribute-Based Access Control Architecture within Large-scale Device Collaboration Systems," *Journal of Networks*, vol. 7, no. 3, pp. 524–531, 2012.

[19] G. Zhang, J. Liu, and J. Liu, "Protecting Sensitive Attributes in Attribute Based Access Control," in *Proc. of the 11th International Conference on Service-Oriented Computing Workshops (ICSOC)*, 2013, pp. 294–305.

[20] R. Sandhu, "The Authorization Leap from Rights to Attributes: Maturation or Chaos?" in *Proc. of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT)*. ACM, 2012, pp. 69–70.

[21] S. Verma, M. Singh, and S. Kumar, "Comparative analysis of Role Base and Attribute Base Access Control Model in Semantic Web," *International Journal of Computer Applications*, vol. 46, no. 18, pp. 1–6, 2012.

[22] E. Coyne and T. R. Weil, "ABAC and RBAC: Scalable, Flexible, and Auditable Access Management," *IT Professional*, vol. 15, no. 3, pp. 14–16, 2013.

[23] X. Jin, R. Krishnan, and R. S. Sandhu, "A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC," in *Proc. of the 26th Conference on Data and Applications Security and Privacy (DBSec)*, 2012, pp. 41–55.

[24] X. Jin, R. S. Sandhu, and R. Krishnan, "RABAC: Role-Centric Attribute-Based Access Control," in *Proc. of the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network (MMM-ACNS)*, 2012, pp. 84–96.

[25] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding Attributes to Role-Based Access Control," *Computer*, vol. 43, no. 6, pp. 79–81, 2010.

[26] B. Morrow, "BYOD Security Challenges: Control and Protect Your Most Sensitive Data," *Network Security*, vol. 2012, no. 12, pp. 5 – 8, 2012.

[27] D. Jana and D. Bandyopadhyay, "Management of Identity and Credentials in Mobile Cloud Environment," in *Proc. of the International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, Sept 2013, pp. 113–118.

[28] E. G. Amoroso, "From the Enterprise Perimeter to a Mobility-enabled Secure Cloud," *IEEE Security&Privacy*, vol. 11, no. 1, pp. 23–31, 2013.

[29] M. Harkins, "A New Security Architecture to Improve Business Agility," in *Managing Risk and Information Security*. Springer, 2013, pp. 87–102.

[30] F. G. Furtmüller, "An Approach to Secure Mobile Enterprise Architectures," *International Journal of Computer Science Issues*, vol. 10, no. 1, pp. 329–336, 2013.

[31] V. Paruchuri and S. Chellappan, "Context Aware Identity Management Using Smart Phones," in *Proc. of the 8th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, 2013, pp. 184–190.

[32] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[33] C. Ngo, P. Membrey, Y. Demchenko, and C. de Laat, "Policy and Context Management in Dynamically Provisioned Access Control Service for Virtualized Cloud Infrastructures," in *Proc. of the 7th International Conference on Availability, Reliability and Security (ARES)*. IEEE, 2012, pp. 343–349.

[34] R. Wu, X. Zhang, G.-J. Ahn, H. Sharifi, and H. Xie, "ACaaS: Access Control as a Service for IaaS Cloud," in *Proc. of the International Conference onSocial Computing (SocialCom)*. IEEE, 2013, pp. 423–428.

[35] D. M. Mangiuc, "Cloud Identity and Access Management A Model Proposal," *Journal of Accounting and Management Information Systems*, vol. 11, no. 3, pp. 484–500, 2012.

[36] J. Gloster, "Efficient Identity Management and Access Control in cloud Environment," in *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2013.

[37] P. Arias-Cabarcos, F. Almenárez-Mendoza, A. Marín-López, D. Díaz-Sánchez, and R. Sánchez-Guerrero, "A Metric-Based Approach to Assess Risk for "On Cloud" Federated Identity Management," *Journal of Network and Systems Management*, vol. 20, no. 4, pp. 513–533, 2012.

[38] M. Dlamini, H. Venter, J. Eloff, and Y. Mitha, "Authentication in the Cloud: A Risk-based Approach," in *Proc. of the 15th annual Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*, 2012.