NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 6, ISSUE 10, Oct.-2019

CLOUD IDENTITY AND ACCESS MANAGEMENT – A MODEL PROPOSAL

Ishaq Azhar Mohammed
Sr. Data Scientist & Department of Information Technology, Dubai, UAE
ishaqazhar14@gmail.com

ABSTRACT

This paper discusses the application of cloud identity and access management in digital transformation and cloud adoption. Cloud computing refers to a fusion of various technologies, including grid computing and distributed computing, that makes use of the Internet as a service delivery network [1]. Organizations need the ability to choose the services and pricing models that best meet their needs, and budgetary constraints. It is the cloud service providers that set the price model for their cloud services, considering factors like instance size, utilization size (per hour), users' size (per user), infrastructure size (per hour), and service size (per service). The majority of businesses are hosting or implementing web services in a cloud infrastructure for the convenience of administration and increased availability [1]. Multi-tenant setups are also utilized in cloud-based services to reduce the cost considerations associated with the services. To accomplish multi-tenancy in the cloud, virtual environments are utilized. A vulnerability in virtual machines poses a direct danger to the privacy and security of the people who are using them [2]. Security problems in cloud web services are found in particular areas such as authentication, authorization, data protection, and accountability, among other things. Cloud security is critical to business and technology sustainability. Even though the "trust boundary" is largely static and monitored and managed by the IT unit in a centralized company where functionality is being implemented within the perimeter of the company, the trust limit becomes dynamic and moves beyond IT command with the adoption of cloud computing [3]. A company's servers, systems, and applications boundaries will expand into the service provider domains. In addition, this loss of control poses a threat to the existing trusted governance and management paradigm, and it has the potential to impede the adoption of cloud services inside an organization if it is not handled correctly. Modern organizations understand the significance of protecting identities in the era of remote work and cloud hosting inside the zero boundaries, Zero Trust. However, as the quantity, kinds, and interrelationships of identities continue to grow exponentially across cloud settings, it is clear that this is a far easier said than done task [3]. Cloud security is widely acknowledged to be a shared duty between cloud service providers and their customers, at least in theory. In the process of determining the best Identity and Access Management (IAM) policies for these settings, many companies are confronted with issues such as: When are cloud-native technologies adequate, and when should we explore specialist solutions from other vendors? With all of the IT security jargon flying about, it may be difficult to discern the difference.

Keywords: Identity and access management, Cloud identity, Cloud IAM, Identity management systems, IT security, IoT, cloud computing

INTRODUCTION

To meet the needs of today's organizations, cloud computing is becoming more essential to them. Cloud web services' current popularity is owing to their accessibility and cost-efficiency. This is accomplished via a variety of customizable service models such as IaaS, SaaS, PaaS, and multi-tenancy. The dangers connected with these service models in terms of privacy and security are significant [4]. To reduce the risks associated with cloud web services, businesses need an Identity and Access Management (IAM) solution that is robust, adaptable, scalable, and responsible to users. The integration of authentication and attribute-based access control improves the performance of the cloud web application by preventing unauthorized access [4,5]. As digital technology continues to develop at a pace without precedents, and the Internet of Things (IoT) is expected to link over 200 billion devices by 2020, companies are facing a fast-changing technological scenario that has dissolved conventional organizational borders. More and more adoption and a rising number of digital identities of different mobile devices are changing business models, social standards, laws, and policy landscape in every industrial company.

As businesses are adapting to these technological advances, many want cloud advantages such as zero+ maintenance (no infrastructure or maintenance expenses other than setup), simplicity of access to the apps, and the freedom to select and utilize the functionalities that suit their operations. On the other hand, heterogeneous landscapes that include on-premises systems, the cloud, and a variety of devices raise several security concerns, especially when it comes to identity and access management [5]. In addition, new and evolving privacy laws often need a review of current procedures to ensure that they remain compliant. Companies need an integrated, consistent, and central strategy to identity management and access control to solve these issues. To assist companies, simplify, optimize, and improve identity and access management spanning on-premise and cloud-based software environments, this article presents SAP Cloud Identity Access Governance. It examines every service that the solution provides and discusses how they are utilized to advance a governance strategy for a company that can be readily tailored to suit changing business requirements.

Many businesses have implemented Identity and Access Management (IAM) systems to reap the many advantages of cloud computing while also mitigating the risks associated with privacy and security concerns. Identity and access management (IAM) is the discipline that ensures that the appropriate people have access to the appropriate resources at the appropriate times and for the appropriate reasons [6]. Aside from that, the IAM systems offer security for sensitive information kept in the cloud, allowing for the dependability and usability of customer access control, which is essential for any organization's website. IAM, on the other hand, is not a panacea, nor does it alleviate all of the privacy and security concerns associated with the cloud. Additionally, distinct identities (or duplicate identities) may be required by various companies within the IAM scope. To solve the issues surrounding identity and access management (IAM), the suggested model of federated identity management (FIM) is presented in this thesis as a method of identity access and management to allow the vision of academic cooperation [6].

PROBLEM STATEMENT

The main problem that this paper will try to solve is an assessment of the relationship between cloud solutions and identity management systems. Despite the many advantages of information and resource sharing, cooperation across different organizations is challenging owing to the complicated involvement of several components [7]. One significant factor is privacy and security concerns, which may prevent universities from sharing their data, even though the usage and access to necessary resources benefit all research facilities. In the most serious circumstances, the stakeholder may steal the technology, abandon the cooperation, and endanger the life of the other stakeholder who shares the technology with them [7,8]. Cooperation is necessary and often essential despite the dangers involved since the shared data may offer the necessary background knowledge on the topic and may help in the formulation of the most appropriate research questions for the benefit of the whole community. Moreover, it may lead to the timely and budget-oriented implementation of major projects which could influence science, creativity, socioeconomic, and employee’s development by leaking classified research information and resources with other parties [8]. To minimize security and privacy problems and to verify resources access for authorized parties, developers propose FIM—a framework that seeks to disguise user identity and confidentiality and enables cooperation with the single sign-in credential, both inside and between enterprises.

LITERATURE REVIEW

A. Identity and Access Management

Identity access management (IAM) is described as the process of controlling who has access to critical information [9]. Information that is designated as "private or protected" may include everything from personal health information to information on credit and debit cards, among other things. All information must be safeguarded from cybersecurity breaches, which include illegal access to systems. It is critical to control who has access to protected data to maintain appropriate cybersecurity practices, even if the information is kept in the cloud. Individual user management (IAM) is concerned with the administration of the roles, access authorizations, and needs of individual users in a corporate IT system. The most important job is to create a digital identity for each person 10]. It is necessary to preserve, update, and monitor a user's identity throughout his or her whole life after it is established. Identity access management is one of the

most important components of maintaining data security in the cloud. Continue reading to find out more about it in this in-depth resource. The practice of storing data on the cloud is becoming more common. Cloud-based systems are easy to use and provide a lot of storage space, but they may also be susceptible to assaults because of their open nature. Hackers are getting access to data in a variety of ways, including via the cloud 10,11]. It is also possible that the platform will make it harder for businesses to control access to the network.

B. Cloud Computing

Cloud computing enables businesses to balance the amount of capacity they need while paying for the services they use every month [12]. When it comes to computer services, cloud computing is a paradigm that allows ubiquitous, practical, on-demand network access to a shared pool of customizable computing resources that can be readily supplied and even released with little administration or participation from service providers. Four deployment types and three service models comprise the Cloud computing model, which is comprised of five major characteristics and five sub-characteristics [12]. Cloud computing aims to accomplish the virtualization of resources while simultaneously increasing the total processing capability of a system. With the introduction of cloud computing, a brand-new standard has been established that allows users to dynamically store or create programs while getting access to them from anywhere and at any time via the use of a network connection. As a result of its ability to provide compute, storage, and software-based services, cloud computing has gained widespread popularity among both businesses and people. Cloud computing helps to alleviate the infrastructure constraint that customers are experiencing by providing pay-per-use apps that are available on-demand [12]. In cloud computing, cloud service providers assume responsibility and execute the necessary functions to operate software and hardware to maximize performance. The commoditization of cloud computing has resulted in a radical type of vertical disintegration, in which physical infrastructure is decoupled from the platform layer and provided as a service.

C. Processes for Identity and Access Management in Cloud Computing

Users may be added, modified, or removed from a cloud computing environment in the same way that they would in a conventional IT system, except for certain minor differences. Before a system's permitted resources may be accessed, users must be added, updated, or deleted from the system. In the conventional approach, identity and access management (IAM) is handled, controlled, and regulated by the company on-premises [13]. Users may access local services such as data and apps by logging in with their username and password. The company that makes use of cloud services is often not in charge of the authentication management process. The vast bulk of authentication takes place on the cloud, which is convenient. Most cloud service providers employ their authentication method to allow customers to access their cloud-based services. In a cloud computing environment, the resources that users may access are determined by the business that is using the cloud computing services. When an organization makes use of cloud services, both the cloud service providers and the companies that make use of cloud services have 9 authorization models that are distinct from one another [13]. Furthermore, since cloud service providers control access to their services, the organization that utilizes cloud services does not have the authority to enforce its security rules against the cloud service providers' services.

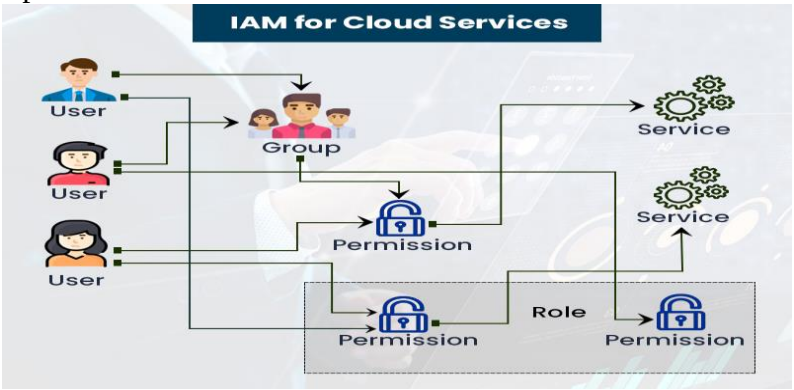

Figure i: IAM for Cloud Services

D. Introduction to Federated Identity

Federated identity management is mainly driven by the need to enhance the user experience and protect personal information. The process of managing users will be simplified thanks to federated identity management. The primary aim of federated identity management is to answer the question of how to utilize an organization's identity management activities to provide direct access to their applications to partners and consumers [14]. Federated identity is the collaborative and interdependent administration of identification information across companies that is referred to as federated identity management. Users from one domain may safely access resources from another domain via the use of the federation paradigm, which eliminates the need for multiple login procedures. Because federated identity management does away with the requirement for users to have an account in the organization directory, they may access services by signing in just one time to the entity that provides their identity management [14].

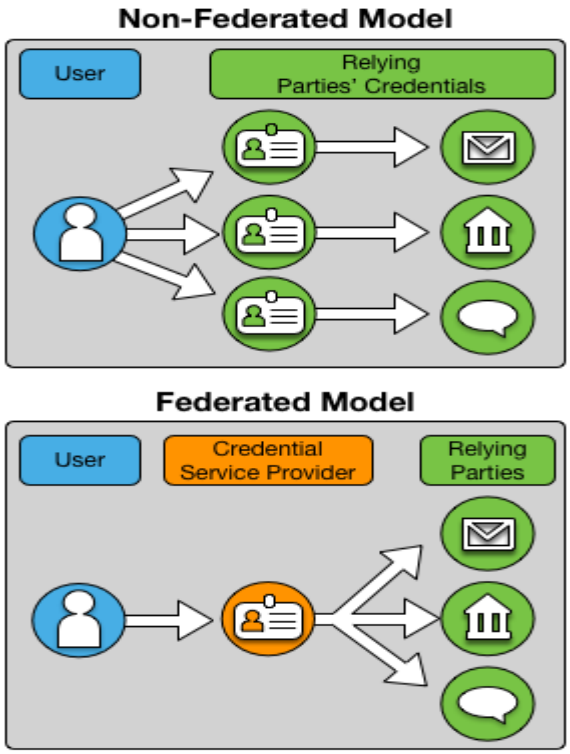

Fig ii: Difference between Federated and non-federated cloud models

E. The CIA Triad as It Applies to Federated Identity

In information security, the CIA Triad (Confidentiality, Integrity, and Availability) is often regarded as the foundational principle [14]. The capacity to establish and execute explicit access limits for information is essential for maintaining confidentiality. In today's environment, people must take steps to safeguard their sensitive and private information from unwanted access. Access control lists, volume and file encryption, and Unix file permissions are just a few of the techniques that are often used to keep information private. Integrity, on the other hand, is designed to prevent data from being deleted or altered without permission [15]. The ability to reverse harm when an authorized person makes a modification that should not have been made is referred to as "integrity." Even while the goal of availability is to safeguard information and make it available when necessary, it is also necessary for authentication procedures, access networks, and systems to operate as intended. Confidentiality is strengthened in the federated identity paradigm in the following ways: third parties do not have plaintext access to user credentials or characteristics, and they will never be able to obtain decryption keys [16]. A hostile man-in-the-middle attack would not compromise the data of an authenticated user, and it would be impossible to obtain unauthorized access to transactional data in such a scenario. Integrity, on the other hand, is strengthened in the following ways: the trusting party has the confidence that the data has not been changed by the hub or a malevolent third party; and When using credential service providers, the relying party may be sure that the data is being supplied by a genuine

credential service provider and that a hostile third party will not impersonate a legitimate user and repeat previously valid claims.

F. The Federated Cloud Identity Broker-Model

In this federated approach, users and service providers do not have to depend on a specific identity broker to function. Both the user and the service provider may rely on their chosen individual broker to complete their transactions [16]. For both the user and the service provider, this eliminates the disadvantage of being dependent on a certain identity broker's accuracy.

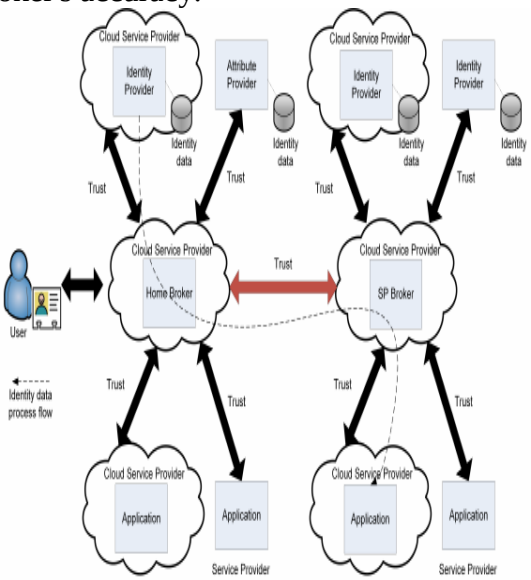

Figure ii: The Federated Cloud Identity Broker-Model

G. Adoption of Cloud Computing and Digital Transformation

With the increasing use of cloud services, the continuous need to stay up with innovation, and the need for every business to create apps, information technology is confronted with a slew of new and difficult issues. It is the goal of today's IT teams to continually enhance efficiency and security for both their internal operations and for end-users, who are the company's customers [16,17]. Any IT manager tasked with modernizing their company has many challenges, including onboarding new workers, managing the many distinct identities lifecycles, and supervising a time-consuming offboarding process that may expose the organization to significant security threats. We provide both on-premises and cloud-based versions of our solutions. Our goods will be adjusted in such a way that they offer a bespoke solution for your company [17].

H. Importance of the proposed model

Federation-based identity management solutions provide individuals more control over the usage and sharing of their identity characteristics across many organizations in the federation. Through the federation of users' identities across several security domains, a user may log in to one domain and then access resources in another domain without having to authenticate again. Users' security may be enhanced as a result of the usage of federated identities. Additional measures such as decreasing and improving authentication processes would help to minimize the likelihood of identity theft occurring. Managing fewer user identities across different apps makes it simpler for an IT administrator to manage fewer user IDs [17,18]. As a result of the many ways of federated login available, users need just one set of login credentials, reducing the amount of administrative work required. There would be no need to deal with the difficulties that new users encounter. It will simply be a matter of providing secure access. Furthermore, there is no longer a need for them to deal with users or identities that are not under their control on an individual basis, resulting in a substantial reduction in the cost of identity life cycle management. Having several login credentials exposes you to a variety of security concerns. A federated login system enables

businesses to overcome this challenge while simultaneously reducing security concerns. Several security measures are made simpler to implement when using federated identity systems.

Authentication is the process of identifying and verifying your identity. Once an identity has been authenticated to a system, authorization defines what resources that identity has access to inside that system. In cloud computing, the combination of a centralized identity, authentication, and permission is a critical component of security. It ensures that only authorized individuals have access to the systems that are required for them to do the activities that are relevant to their position in the company [18]. On the other hand, it provides for the auditing of system modifications and the tracking of changes back to particular individuals. When developing an identity and access management system for your company, it is becoming more essential to have efficient procedures in place so that your staff can concentrate on their real job. The fact that cloud platforms frequently come with basic rules that are intended to prevent unwanted access to data does not mean that these controls are sufficient for protecting the personal information of customers. There are several additional measures that businesses may take to ensure data security while still benefiting from the ease of cloud-based storage [18].

The Challenges and Risks of Identity and Access Management Programs in Cloud Computing

Implementing an IAM program has many benefits, but it also comes with dangers and difficulties, which must be taken into consideration. One of the most significant dangers is relying on identity and access control software to prevent unauthorized usage of the system, which is one of the most common scenarios. This is the most pressing issue for many large and small businesses alike. If the access controls are broken, hackers may be able to roam freely across the network without being detected [18]. This might involve gaining access to confidential or protected information (PPI). This is especially true with cloud computing, where the danger is higher. If there are more access points, it may be simpler for hackers to penetrate the system if the identity authentication procedures are not efficient and effective. Many companies are faced with a difficult task when attempting to establish an IAM program. According to the scale and breadth of the project, it may take a long time and be very costly. Company IT teams may be slowed down for weeks while adopting the procedures. Other cybersecurity procedures may be permitted to slip for a short period during this period [18]. This may be seen as an encouragement for hackers to take advantage of a flaw. Professionals in the field of cybersecurity may assist companies in the implementation of an identity and access management program. In this way, the IT staff will be able to continue to monitor the current procedures. Despite the dangers and difficulties, the advantages of implementing an IAM program exceed any possible drawbacks.

FUTURE IN US IT SECTOR

Several businesses in the United States are reconsidering their conventional methods to maintaining their digital identities as a result of the continuing development of cloud-based services. As businesses migrate their business operations to the cloud, organizations must control access to and inside cloud service providers' networks. Identity service hosting locations are becoming less important as more companies use Zero Trust security concepts, such as ID verification and network context restrictions, as part of their overall security strategy. Identity management services are provided by cloud infrastructure companies such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud as a matter of necessity [18]. External-facing apps operating on hosting cloud infrastructures need the complete support of the OpenID Connect (OIDC) architecture from the cloud infrastructure provider to back cloud services with a rich user interface. Internal and external identity services are two of the most basic aspects of cloud identity services [18,19]. Future use cases and cost advantages will develop, but they will most likely only be accessible to companies that have strong cloud identity policies that rely on verifiable procedures to trust external entities and events in the first place. Identity as a service offers the greatest path ahead for the majority of businesses seeking to position themselves for long-term success.

ECONOMIC BENEFITS

The continued growth of the Internet economy in the United States is dependent on the proper management of online identification information. When it comes to identity management, it is essential in a variety of

settings, including the enterprise, e-commerce, and government, since it underpins corporate operations and services, as well as enabling digital interactions and transactions from the viewpoint of the consumer. Enterprises and their network customers benefit from identity federation since it provides both economic and convenience benefits [19]. For example, several companies may pool their resources to use a single application, leading to cost savings and resource consolidation. Organizations collaborating on a project may establish an identity federation to make it easier for all of its users to access and share resources throughout the organization [19]. As a result, users only need to log in once to share information across all domains, but administrators at each organization may still manage the degree of access to resources inside their respective domains. This strategy has the potential to save money while also consolidating resources.

CONCLUSION

The main aim of this paper was to research and get an understanding of how cloud solutions may be used in the field of identity and access management (IAM). There are many advantages to using the cloud, including lower prices and shorter delivery times for solutions and data sharing. Federated identity is a component of this revolution that is still in its early stages. This study investigates ways to take advantage of cloud services, namely federated identity, as a critical element in enabling cooperation across companies on cloud computing projects. As opposed to the conventional IAM architecture, users and service providers in FIM may be authorized using their chosen cloud identity broker. This new feature in FIM lowers the cost of user management while also streamlining the integration of security and the user experience for the user. Even though the identity broker may person attributes privacy issues, and identification environment of federated identity options can play a critical role in acquiring more secure cyberspace by prohibiting identity providers from acquiring access to users' identities and other personal information. When it comes to computer resources, cloud computing is a platform that delivers easy, on-demand demand access to a shared stream of customizable resources. Such resources refer to different networks, servers, storage facilities, apps, and services that are quickly delivered and distributed with minimum administrative effort or contact across cloud providers. In addition to increasing availability, accountability, and scalability, cloud computing offers the potential to deliver a more cost-effective environment via optimization and more efficient processing. Data centers or cloud infrastructures are supplied and managed by companies or third-party suppliers, depending on the context. As a computational paradigm and a distribution architecture, cloud computing's primary goal is to offer safe, fast, and easy storage space as well as network computing capabilities, with all computer resources represented as services and supplied via the Internet.

REFERENCES

1) J. Nickel, Mastering Identity and Access Management with Microsoft Azure. Birmingham, UK: Packt Publishing, 2016.
2) A. Hietajärvi and K. Aaltonen, "The formation of a collaborative project identity in an infrastructure alliance project", Construction Management and Economics, vol. 36, no. 1, pp. 1-21, 2017.
3) G. Goth, "Identity management, access specs are rolling along", IEEE Internet Computing, vol. 9, no. 1, pp. 9-11, 2005.
4) G. Kecskemeti, A. Kertesz and Z. Nemeth, Developing interoperable and federated cloud architecture. Hershey, Pennsylvania: IGI Global, 2016.
5) T. Hunter, Google Cloud Platform for developers : build highly scalable cloud solutions with the power of Google Cloud Platform. PACKT Publishing Limited, 2018.
6) M. Uddin and D. Preston, "Systematic Review of Identity Access Management in Information Security", Journal of Advances in Computer Networks, vol. 3, no. 2, pp. 150-156, 2015.
7) Å. Grönlund, "Electronic identity management in Sweden: governance of a market approach", Identity in the Information Society, vol. 3, no. 1, pp. 195-211, 2010.
8) S. Bawazir, P. Sofotasios, S. Muhaidat, Y. Al-Hammadi, and G. Karagiannidis, "Multiple Access for Visible Light Communications: Research Challenges and Future Trends", IEEE Access, vol. 6, pp. 26167-26174, 2018.

9) O. Maslak, N. Grishko, K. Vorobiova, O. Hlazunova, and M. Maslak, "Developing the intra-firm technology transfer system at the industrial enterprise based on matrix approach", Problems and Perspectives in Management, vol. 15, no. 3, pp. 242-252, 2017.
10) C. Chinedu Anyaoku, "The Future Of Municipal Solid Waste Management", Science Trends, 2018.
11) R. Holley, "Open Access: Current Overview and Future Prospects", Library Trends, vol. 67, no. 2, pp. 214-240, 2018.
12) S. Bawazir, P. Sofotasios, S. Muhaidat, Y. Al-Hammadi and G. Karagiannidis, "Multiple Access for Visible Light Communications: Research Challenges and Future Trends", IEEE Access, vol. 6, pp. 26167-26174, 2018.
13) M. Schwartz and M. Machulak, Securing the perimeter : deploying identity and access management with free open source software. New York: Apress, 2018.
14) T. Ryzhakina, N. Koroleva and N. Makasheva, "A process-based approach to the management of the enterprise", SHS Web of Conferences, vol. 28, p. 01088, 2016.
15) J. Balmer and S. Greyser, "Managing the Multiple Identities of the Corporation", California Management Review, vol. 44, no. 3, pp. 72-86, 2002.
16) L. Martin, "Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management", Information Systems Security, vol. 16, no. 1, pp. 9-14, 2007.
17) E. Zavadskas, A. Kaklauskas, M. Gikys and N. Lepkova, "A multiple criteria decision support web-based system for facilities management", International Journal of Internet and Enterprise Management, vol. 2, no. 1, p. 30, 2004.
18) E. Damiani, S. De Capitani diVimercati and P. Samarati, "Managing multiple and dependable identities", IEEE Internet Computing, vol. 7, no. 6, pp. 29-37, 2003.
19) K. Flieder, "Identity- und Access-Management mit EAI-Konzepten und -Technologien", Datenschutz und Datensicherheit - DuD, vol. 32, no. 8, pp. 532-536, 2008.