International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(1), pp.300-308
DOI: http://dx.doi.org/10.21172/1.81.039
e-ISSN:2278-621X

IDENTITY AND ACCESS MANAGEMENT: CONCEPT, CHALLENGES, SOLUTIONS

Mayuri Dhamdhere[1] and Sridevi Karande[2]

Abstract: Identity and Access Management is important in today's evolving world. It is the process of managing who has access to what information over time. Activity of IAM involves creation of identities for user and system. Secure user access plays a key role in the exchange of data and information. In addition, electronic data is becoming ever more valuable for most companies. Access protection must therefore meet increasingly strict requirements – an issue that is often solved by introducing strong authentication. Identity and the Access are two very important concept of the IAM which are needed to be managed by the company. Companies are now relying more on the automated tool which can manage all these things. But then it creates the risk. Because tools are not intelligent enough to take the decisions, so we can add the intelligence by using the various data mining algorithm. This can keep the data over time and then build the models. This paper covers all the challenges associated with the Identity and Access Management. The possible solution is given for these challenges.

I. INTRODUCTION

Currently, companies are more and more concerned in complex value chains also they necessary to both integrate and offer a range of information systems. As a result of this, the lines among service providers and users and among competitors are blurring. Companies therefore need to implement efficient and flexible business processes focused on the electronic exchange of data and information. Such processes require reliable identity and access management solutions. IAM is the process which manages who has access to what information over time. Activity of IAM involves creation of identities for user and system. Identity and Access Management IAM has recently emerged as a critical foundation for realizing the business benefits in terms of cost savings, management control, operational efficiency, and, most importantly, business growth for ecommerce. Enterprises need to manage access to information and applications scattered across internal and external application systems. Moreover, they must provide this access for a growing number of identities, both inside and outside the organization, without compromising security or exposing sensitive information. IAM comprises of people, processes and products to manage identities and access to resources of an enterprise. An identity access management (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management. IAM technology can be used to initiate, capture, record and manage user identities and their related

[1] *Department of Computer Engineering MIT, Pune*
[2] *Department of Computer Engineering MIT, Pune*

access permissions in an automated fashion. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited. Poorly controlled IAM processes may lead to regulatory non-compliance because if the organization is audited, management will not be able to prove that company data is not at risk for being misused

Additionally, the enterprise shall have to ensure the correctness of data in order for the IAM Framework to function properly. IAM components can be classified into 4 major categories: authentication, authorization, user management and central user repository (Enterprise Directory). The ultimate goal of IAM Framework is to provide the right people with the right access at the right time. See below diagram

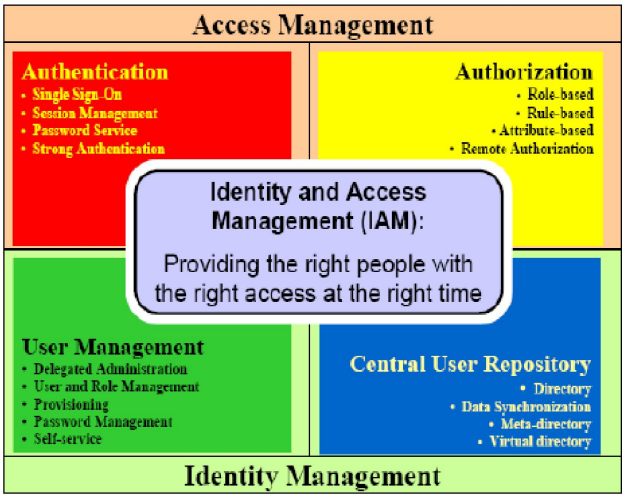

Figure 1: What is Identity Management

Authentication

This area is comprised of authentication management and session management. Authentication is the module through which a user provides sufficient credentials to gain initial access to an application system or a particular resource. Once a user is authenticated, a session is created and referred during the interaction between the user and the application system until the user logs off or the session is terminated by other means (e.g. timeout). The authentication module usually comes with a password service module when the user Id / password authentication method is used. By centrally maintaining the session of a user, the authentication module provides Single Sign-On service so that the user needs not logon again when accesses another application or system governed under the same IAM Framework.

Authorization

Authorization is the module that determines whether a user is permitted to access a particular resource. Authorization is performed by checking the resource access request, typically in the form of an URL in web-based application, against authorization policies that are stored in an IAM policy store. Authorization is the core module that implements role-based access control. Moreover, the authorization model could provide complex access controls based on data or information or policies including user attributes, user roles / groups, actions taken, access channels, time, resources requested, external data and business rules.

User Management

This area is comprised of user management, password management, role/group management and user/group provisioning. User management module defines the set of administrative functions such as identity creation, propagation, and maintenance of user identity and privileges. One of its components is user life cycle management that enables an enterprise to manage the lifespan of a user account, from the initial stage of provisioning to the final stage of de-provisioning. Some of the user management functions should be centralized while others should be delegated to end-users. Delegated administration allows an enterprise to directly distribute workload to user departmental units. Delegation can also improve the accuracy of system data by assigning the responsibility of updates to persons closest to the situation and information. Self-service is another key concept within user management. Through self-profile management service an enterprise benefits from timely update and accurate maintenance of identity data. Another popular self-service function is self-password reset, which significantly alleviates the help desk workload to handle password reset requests. User management requires an integrated workflow capability to approve some user actions such as user account provisioning and de-provisioning.

Central User Repository

Central User Repository stores and delivers identity information to other services, and provides service to verify credentials submitted from clients. The Central User Repository presents an aggregate or logical view of identities of an enterprise. Directory services adopting LDAPv3 standards have become the dominant technology for Central User Repository. Both Meta-directory and Virtual directory can be used to manage disparate identity data from different user repositories of applications and systems. A meta-directory typically provides an aggregate set of identity data by merging data from different identity sources into a meta-set. Usually it comes with a 2-way data synchronization service to keep the data in sync with other identity sources. A virtual directory delivers a unified LDAP view of consolidated identity information, behind the scene multiple databases containing different sets of users are combined in real time.

1.1. Need of IAM

Secure user access plays a key role in the exchange of data and information. In addition, electronic data is becoming ever more valuable for most companies. Access protection must therefore meet increasingly strict requirements – an issue that is often solved by introducing strong authentication. Modern IAM solutions allow administering users and their access rights flexibly and effectively, enabling multiple ways of cooperation. Also, IAM is a prerequisite for the use of cloud services, as such services may involve outsourcing of data, which in turn means that data handling and access has to be clearly defined and monitored. At the same time, companies are facing the challenge of having to work with various forms of IAM data provided by historically grown systems. To be able to meet current security requirements and react quickly if required, they need to identify and consolidate such data sources and define a data lifecycle. In general, IAM tasks can be divided into three levels, as illustrated in the diagram on the right. The governance level defines the regulatory framework and the compliance and review procedures. The management level allows administration of identities, rights and authorization tokens. The execution level ensures information review as well as synchronization at runtime.

It can be difficult to get funding for IAM projects because they don’t directly increase either profitability or functionality. However, a lack of effective identity and access management poses

significant risks not only to compliance but also an organization's overall security. These mismanagement issues increase the risk of greater damages from both external and inside threats.

Keeping the required flow of business data going while simultaneously managing its access has always required administrative attention. The business IT environment is ever evolving and the difficulties have only become greater with recent disruptive trends like bring-your-own-device (BYOD), cloud computing, mobile apps and an increasingly mobile workforce. There are more devices and services to be managed than ever before, with diverse requirements for associated access privileges. With so much more to keep track of as employees migrate through different roles in an organization, it becomes more difficult to manage identity and access. A common problem is that privileges are granted as needed when employee duties change but the access level escalation is not revoked when it is no longer required. This situation and request like having access like another employee rather than specific access needs leads to an accumulation of privileges known as privilege creep. Privilege creep creates security risk in two different ways. An employee with privileges beyond what is warranted may access applications and data in an unauthorized and potentially unsafe manner. Furthermore, if an intruder gains access to the account of a user with excessive privileges, he may automatically be able to do more harm. Data loss or theft can result from either scenario.

Typically, this accumulation of privilege is of little real use to the employee or the organization. At best, it might be a convenience in situations when the employee is asked to do unexpected tasks. On the other hand, it might make things much easier for an attacker who manages to compromise an over-privileged employee identity. Poor identity access management also often leads to individuals retaining privileges after they are no longer employees.

II. CONCEPT OF IDENTITY AND ACCESS MANAGEMENT

Definition of Key concept

1. Identity

The element or combination of element that uniquely describes a person or machines is called Identity. It can be what you know such as password or other personal information what you have or any combination of these.

2. Access

The information representing the rights that identity was granted. This information the access rights can be granted to allow users to perform transactional functions at various levels. Some examples of transactional functions are copy, transfer, add, change, delete, review, approve and cancel.

3. Entitlements

The collection of access rights to perform transactional functions is called entitlements. The term entitlements are used occasionally with access rights.

Identity and access management is the, who, what, where, when, and why of information technology. It encompasses many technologies and security practices, including secure single sign-on (SSO), user provisioning/de provisioning, authentication, and authorization. Over the past several years, the Fortune 2000 and governments worldwide have come to rely on a sound IAM platform as the foundation for their GRC strategies. This is borne out by the numbers: IDC

research shows that the IAM market accounted for almost $4 billion in license and maintenance revenue in 2010, and we estimate that 80% of these sales were directly driven by the need to meet regulatory compliance mandates.

This lays the foundation for the larger GRC infrastructure for the enterprise, an area where companies such as SAP and NetIQ (and Novell before it) have combined years of experience and expertise. IDC defines GRC infrastructure as focusing on solutions that provide policy and workflow definition; documentation; policy enforcement and operationalization; and monitoring, testing, and verification of controls at the IT infrastructure layer. It is an ongoing, dynamic process. As more organizations decentralize with branch and home offices, remote employees, and the consumerization of IT, the need for strong security and GRC practices is greater than ever.

III. FUNCTION OF IDENTITY MANAGEMENT

The identity management system stores information on all aspects of the identity management infrastructure. Using this information, it provides authorization, authentication, user registration and enrolment, password management, auditing, user self-service, central administration, and delegated administration.

• Stores information

The identity management system stores information about the following resources: applications (e.g. business applications, Web applications, desktop applications), databases (e.g. Oracle, DB2, MS SQL Server), devices (e.g. mobile phones, pagers, card keys), facilities (e.g. warehouses, office buildings, conference rooms), groups (e.g. departments, workgroups), operating systems (e.g. Windows, Unix, MVS), people (e.g. employees, contractors, customers), policy (e.g. security policy, access control policy), and roles (e.g. titles, responsibilities, job functions).

• Authentication and authorization

The identity management system authenticates and authorizes both internal and external users. When a user initiates a request for access to a resource, the identity management first authenticates the user by asking for credentials, which may be in the form of a username and password, digital certificate, smart card, or biometric data. After the user successfully authenticates, the identity management system authorizes the appropriate amount of access based on the user's identity and attributes. The access control component will manage subsequent authentication and authorization requests for the user, which will reduce the number of passwords the user will have to remember and reduce the number of times a user will have to perform a logon function. This is referred to as "single sign-on" or "reduced sign-on." A realistic goal for an identity management system is to enable single sign-on for all Web applications, but it is currently unrealistic to provide single sign-on functionality for all applications across the enterprise.

• External user registration and enrolment

The identity management system allows external users to register accounts with the identity management system and also to enrol for access privileges to a particular resource. If the user cannot authenticate with the identity management system the user will be provided the opportunity to register an account. Once an account is created and the user successfully authenticates, the user must enrol for access privileges to requested resources. The enrolment

process may be automated based on set policies or the owner of the resource may manually approve the enrolment. Only after the user has successfully registered with the identity management system and enrolled for access will access to that resource be granted.

• Internal user enrolment

The identity management system allows internal users to enroll for access privileges. Unlike external users, internal users will not be given the option to register because internal users already have an identity within the identity management system. The enrolment process for internal users is identical to that of external users.

• Auditing

The identity management system facilitates auditing of user and privilege information. The identity management system can be queried to verify the level of user privilege. The identity management system provides data from authoritative sources, providing auditors with accurate information about users and their privileges.

• Central administration

The identity management system allows administrators to centrally manage multiple identities. Administrators can centrally manage both the content within the identity management system and the structural architecture of the identity management system.

IV. CHALLENGES IN IDENTITY AND ACCESS MANAGEMENT

Today's enterprise IT departments face the increasingly complex challenge of providing granular access to information resources, using contextual information about users and requests, while successfully restricting unauthorized access to sensitive corporate data.

1. An increasingly distributed workforce

One way organizations can recruit and retain the best talent is to remove the constraints of geographic location and offer a flexible work environment. A remote workforce allows businesses to boost productivity while keeping expenses in Check as well as untethering employees from a traditional office setting. However, with employees scattered all over a country or even the world, enterprise IT teams face a much more daunting challenge: maintaining a consistent experience for employees connecting to corporate resources without sacrificing security. The growth of mobile computing means that IT teams have less visibility into and control over employees' work practices. Solution is, a comprehensive, centrally managed IAM solution returns the visibility and control needed for a distributed workforce to an enterprise IT team.

2. Distributed applications

With the growth of cloud-based and Software as a Service (SaaS) applications, users now have the power to log in to critical business apps like Salesforce, Office365, Concur, and more anytime, from any place, using any device. However, with the increase of distributed applications comes an increase in the complexity of managing user identities for those applications. Without a seamless way to access these applications, users struggle with password management while IT is faced with rising support costs from frustrated users. Solution is a

holistic IAM solution can help administrators consolidate, control, and simplify access privileges, whether the critical applications are hosted in traditional data centers, private clouds, public clouds, or a hybrid combination of all these spaces.

3. Productive provisioning

Without a centralized IAM system, IT staff must provision access manually. The longer it takes for a user to gain access to crucial business applications, the less productive that user will be. On the flip side, failing to revoke the access rights of employees who have left the organization or transferred to different departments can have serious security consequences. To close this window of exposure and risk, IT staff must de-provision access to corporate data as quickly as possible. Unfortunately, in many organizations this means that IT has to go through each user's account to understand what resources they have access to and then to manually revoke that access. Manual provisioning and de provisioning of access is labor intensive and prone to human error or oversights. Especially for large organizations, it is not an efficient or sustainable way to manage user identities and access. Solution is the a robust IAM solution can fully automate the provisioning and de-provisioning process, giving IT full power over the access rights of employees, partners, contractors, vendors, and guests. Automated provisioning and de provisioning speed the enforcement of strong security policies while helping to eliminate human error.

4. Bring your own device (BYOD)

To manage or not to manage—there really is no choice between the two for today's enterprises. Employees, contractors, partners, and others are bringing in personal devices and connecting to the corporate network for professional and personal reasons. The challenge with BYOD is not whether outside devices are brought into the enterprise network, but whether IT can react quickly enough to protect the organization's business assets—without disrupting employee productivity and while offering freedom of choice. Nearly every company has some sort of BYOD policy that allows users to access secure resources from their own devices. However, accessing internal and SaaS applications on a mobile device can be more cumbersome than doing so from a networked laptop or desktop workstation. In addition, IT staff may struggle to manage who has access privileges to corporate data and which devices they're using to access it. Solution is enterprises must develop a strategy that makes it quick, easy, and secure to grant—and revoke—access to corporate applications on employee- and corporate-owned mobile devices based on corporate guidelines or regulatory compliance. In addition, technology shifts such as the trend toward an Internet of Things requires corporate IT teams to deploy solutions that can scale to meet the onslaught of devices looking to tax the corporate network.

5. Password problems

The growth of cloud-based applications means that employees must remember an increasing number of passwords for applications that may cross domains and use numerous different authentication and attribute-sharing standards and protocols. User frustration can mount when an employee spends more and more time managing the resulting lists of passwords which, for some applications, may require changing every 30 days. Plus, when employees have trouble with their passwords, they most often contact IT staff for help, which can quickly and repeatedly drain important resources. Solution is Enterprises can readily make password issues a thing of the past by federating user identity and extending secure single sign-on (SSO) capabilities to SaaS, cloud-

based, web-based, and virtual applications. SSO can integrate password management across multiple domains and various authentication and attribute-sharing standards and protocols.

6. Regulatory compliance

Compliance and corporate governance concerns continue to be major drivers of IAM spending. For example, much of the onus to provide the corporate governance data required by Sarbanes-Oxley regulations falls on the IT department. Ensuring support for processes such as determining access privileges for specific employees, tracking management approvals for expanded access, and documenting who has accessed what data and when they did it can go a long way to easing the burden of regulatory compliance and ensuring a smooth audit process. Solution is a strong IAM solution can support compliance with regulatory standards such as Sarbanes-Oxley, HIPAA, and the payment card industry data security standards (PCI DSS). In particular, a solution that automates audit reporting can simplify the processes for regulatory conformance and can also help generate the comprehensive reports needed to prove that compliance.

V. CONCLUSION AND FUTURE WORK

Efficiency, Security and Compliance are important keys of Identity and Access Management. Benefits of deploy a vigorous IAM solution are clear, the complexity and cost of implementation can disrupt even the most well-intentioned organization. But, when enterprise consider the cost of a possible security breach or study the inefficiencies intrinsic to the manual provisioning and de-provisioning of contact to corporate resources, the imperative is clear: However It is the time to build a federal IAM team that can build and implement organization-wide identity and access management policies. The conventional security perimeter is shrinking. Enterprises searching for IAM solutions must take into explanation the realities of an increasingly mobile workforce and a highly distributed and difficult network of applications. A robust IAM solution can ease organization pains, streamline provisioning and de-provisioning, and improve user productivity, while lowering costs, dropping demands on IT, and providing the enterprise with comprehensive data to assist in complying with regulatory standards. Also enterprises can make sure security by deploying solutions with strong authentication and authorization, while remove user frustration by delivering seamless access to cloud-based applications through Single sign on. In addition, as identity and access management becomes more and more complex, the ability to create policies based on contextual and granular information will become more important. IAM solutions that can gather and make decisions based on user identity, devise, location, and the requested resource will allow enterprises to distribute quick access to employees, partners, and contractors. Also they can deny privileges to unauthorized users.

REFERENCES

[1]. Matthias Hummer, Michael Kunz: 2015 IEEE, “Advanced Identity and Access Policy Management using Contextual Data”, 978-1-4673-6590-1/15

[2]. Sebastian Ryszard Kruk, Slawomir Grzonkowski, Adam Gzella: 2006 Springer,“D-FOAF: Distributed Identity Management with Access Rights Delegation”, LNCS 4185, pp. 140–154.

[3]. Marco Casassa Mont, Siani Pearson, Pete Bramhall: 2003 IEEE,” Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services”, 1529-4188/03.

[4]. Robert Cowles: 2013 IEEE,”Identity Management for Virtual Organisation”, 978-0-7695-5083-1/13

[5]. Ludwig Fuchs, Günther Pernul: 2007 IEEE. “Supporting Compliant and Secure User Handling - A Structured Approach for In-House Identity Management” , 0-7695-2775-2/07

[6]. Anat Hovav: 2009, “Communications of the Association for Information Systems”, Volume 25 | Number 1 Article 42

[7]. Ian Jacobi, Daniela Miao: 2013 IEEE," Transitioning Linked Data Accountable Systems to the Real World with Identity, Credential, and Access Management (ICAM) Architectures", 978-1-4799-1535-4/13

[8]. Cees B.M. van Riel: 2007, "Corporate identity: the concept, its measurement and management", European Journal of Marketing 31, 5/6.

[9]. Frank Schell, Andreas Schaf: 2010 ACM, "Assessing Identity and Access Management Systems Based on Domain-Specific Performance Evaluation", WOSP/SIPEW'10, January 28–30

[10]. The Challenges and Benefits of Identity and Access Management, 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

[11]. "Identity and Access Management" https://books.google.co.in/books?id=nWtAAAAQBAJ&printsec=frontcover#v=onepage&q&f=false https://en.wikipedia.org/wiki/Identity_management http://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system