Identity Management Systems: A Comparative Analysis

Vikas Kumar, School of Business Studies, Sharda University, Greater Noida, India
Aashish Bhardwaj, Mewar University, Chittorgarh, India

ABSTRACT

This article describes how in today’s digital world, customers have made it a common practice to maintain user accounts with different service providers to access a range of services. In such environment, all attributes of the identity must be verified to operate, otherwise the resources would be vulnerable to financial and data loss. This article contends that makes it important to form an Identity Management System, which could provide central administration, user self-service, role based access control and integrated user management. Identity Management becomes very much vital for the environment working with multiple technologies, as it governs an entity (i.e. a human or a software agent) to authenticate and authorize for accessing the network via multiple technologies. Successful Identity Management increases the efficiency, security, access control and decreases the complexity, cost and many repetitive works. Essential features of present day identity management systems have been identified in the present work. A comparative analysis of these identity management systems has been carried out to establish the present-day industry practices. Along with that, specific challenges to the present-day identity management systems have been identified. The article helps in the identification of suitable Identity Management System for specific applications.

KEYWORDS

Customers, Identity Management System, Security, User Self-Service

1. INTRODUCTION

As the world population is increasing, number of Internet users, mobile phone users and email users is also increasing. World population clock, worldometer (2017) has calculated world population as 7.51 billion, whereas it was merely 3.68 billion in 1970. There has been an appreciable increase in the number of email users as well. As per the Email Statistics Report (Team, 2015), email users throughout the world are increasing at a rate of 3% since 2015 but Email accounts are increasing at 6% - 7% every year since 2015 (Team, 2015). This has been a trend to have multiple email accounts by individuals for personal reasons. A valid email account is primary requirement for all online transactions like shopping, banking, social networking etc., which drives the way for having multiple email accounts. Email accounts are not only used for interpersonal communication but also for many other online notifications and transactions as well. On the other hand, mobile phones have become an integral part of the society and they are serving as the primary technology interface, rather than being a mere communication device. There has been an unprecedented increase in the number of mobile phone users worldwide. Mobile phone users will reach 5.07 billion in 2019 from 4.77 billion in 2017 (Statista, 2017). This has steadily increased from 4.01 billion in 2013 to 4.61 billion in 2016.

DOI: 10.4018/IJSDS.2018010105

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
As per Internet World Stats (2017), penetration rate of Internet will reach 49.7% world-wide. This further leads to the increase in number of internet based applications.

Social media has emerged as another popular tool and large amount of personal information flows on internet via social media. This includes person’s profile photo, name, contact number, address and other personal details. All these are enough for a criminal to steal the identity of a person. Even though authorities are also vigilant for these thefts and are using different means to prevent these incidents to happen. Around the world, police is actively conducting surveillance and investigations for years to prevent incidents of identity theft. Even after that, the identity theft incidents are not stopping and many public politicians and figures fear such an impersonation attack. Many specific cases of social media and identity theft have been presented by Socialnomics (2016). The 2017 Identity Fraud Study (Javelin Strategy & Research, 2017) revealed that the identity fraud incidence rate has increased by 16% from 2015 to 2016 in United States. The study also found that fraudsters have successfully targeted two million more victims this year and the theft has amounted to $16 billion. This study has also found that fraudsters are moving to the online platforms and Card-not-present (CNP) fraud is significantly increasing. As the microchip equipped credit cards got introduced in United States in 2015, these cards are difficult to counterfeit. Hence, the criminals focused on new account fraud, where a fraudster opens a credit card or other financial account using a victim’s name and other stolen personal information. These show a very typical case of identity theft. Also, in 2016, thirteen percent of all complaints received by the Federal Trade Commission (USA) were related to identity theft (https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime).

Identity Management and Identity & Access Management are terms used interchangeably and lay under Security and threat assessment services (Singh & Kumar, 2013; Pradhan & Kumar, 2016). Identity management (IdM) describes the management of individual identities, their authentication, authorization, roles and privileges within organization or across boundaries (Marmol, 2010; Karopoulos, 2010; De Hert, 2008; ClauB, 2001). The Identity and Access management is a term that refers to administration of individual identities within a system, as a company, a country or even a network. In an information technology company, identity management is used to establish and manage the roles and access privileges of individual users of the network. The identity management systems provide decision makers with tools and technologies to control user access to critical information within the organization. Main functionality of Identity management system is to increase security and productivity, while decreasing the cost, downtime and repetitive tasks. These include user creation, user deletion, lock user, unlock user, grant access, and revoke access (Zissiz & Lekkas, 2012; Vrhovec, 2011 and Misra & Mondal, 2011). Users with excessive rights in a system can lead to losses for business from a security point of view. Improved security guarantees that authenticated users have access to information and are doing things correctly (Chonka et al., 2011; Taylor et al., 2010 and Svantesson & Clarke, 2010).

Unique Identification for individuals across the world is difficult to implement because of privacy reasons. More than 80 countries in the world have formulated laws on protecting privacy of their citizens. These are mostly part of information security or data protection acts of the country. Users keep on multiplying in the present-day mobile, internet and cloud computing environment. Organizations can manage business risks by using the efficient Identity management system, however the cost remains a prime demerit of Identity Management as technology needs to be continuously upgraded to take care of these increasing needs. In this new era of computing, organizations need to identify ways to manage risks for their business and growth. Many researchers have presented the challenges of cloud adoption to organizations, service providers as well as governments (Singh & Kumar, 2014; Vidhyalakshmi & Kumar, 2014 and Pradhan & Kumar, 2016). There are different user & business challenges for identity and access management which impacts a wide range of functions in every organization (http://hitachi-id.com/concepts/websso.html). Backbone of any business is the agility and taking advantages of new opportunities, so that benefits can be transferred to customers.
A Decision Support System for On-Demand Goods Delivery Using Shared Autonomous Electric Vehicles
www.igi-global.com/article/a-decision-support-system-for-on-demand-goods-delivery-using-shared-autonomous-electric-vehicles/223428?camid=4v1a

A Mediator for Biospatial Information Systems
www.igi-global.com/article/mediator-biospatial-information-systems/3898?camid=4v1a