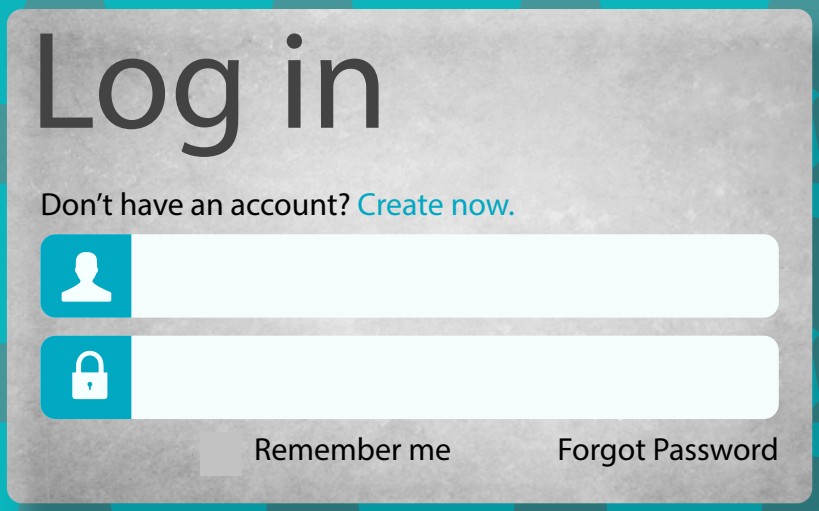
happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

User Identity: A Centric Approach



Happiest People . Happiest Customers

Contents

Introduction

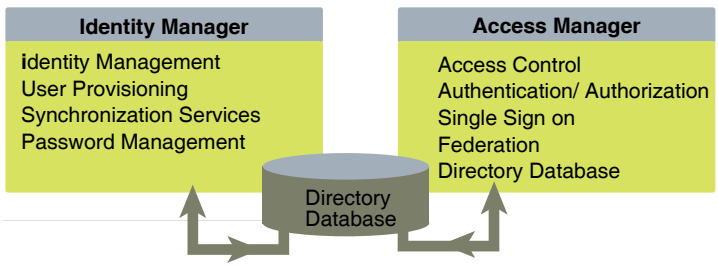
User Identity Management (IdM) is a complex and constantly evolving practice of identifying individuals and controlling their access through networks and connected systems. IdM research focuses primarily on making systems secure, while the quality of the user experience is largely ignored. This article explores reasons why creating a user-centric identity solution has become necessary and discusses existing efforts to make IdM more user centric presenting one possible implementation of user centric IdM that, in theory, could leverage mobile devices and support both, On-Premise and Cloud infrastructure.

About Identity & Access Management

The internet has quickly become a convenient meeting place for corporate people, including employees, contractors, customers, partners and vendors. Multiple devices/systems make the interaction between these groups possible for communication and exchanging the data. Just imagine how many people are accessing or connecting with your own network to begin with! Do you know who they are, where they are and what they are doing on your network? The answer would be “No”!

Here we are talking about User Identity and Access management. Identity Management centralizes control over user’s identity within the network. Its delegated workflows, rules and policies allow for automated provisioning and user self-service. Identity Management involves a process of creating user accounts that can modify and regulate the interaction a user has with the network. Relationships between the user and their role with the business are established through various rules and policies. The rules and policies identify what resources the user has access to. Assigning authorizations and permissions define the 3-W of network use (when, where and why). Whereas, Access Management centralizes the control over user’s rights or access within the network. In other words, what it does is provide Single Sign-On (SSO) capability to have seamless access on the network resources and applications.

Let us understand the concept of Identity and Access management using the below:



The above figure shows the Identity Manager, Access Manager and Directory Server Identity management components. Identity Manager provides user provisioning, password management, synchronization services, comprehensive audit & reporting, and delegated administration, while Access Manager generates user Authentication, Authorization, Single Sign-on and Federation services.

There are many Identity & Access Management (IAM) tools available in the market for user identity management. It depends which IAM product suite is well suitable for your organization's business stories.

As many daily tasks become available into the capabilities of modern mobile smartphones (Android, iOS, Blackberry, etc.) such as Email, Calendar Management, Online Shopping, Social Networking and Financial Transactions, the lives of technology-enabled users are increasingly centered on their mobile devices. Increasingly smartphones has very important & vital role in our lives.

In centralized user identity models, there exists a single identifier and credentials provider that is used by all service providers (applications), either exclusively, or in addition to other identifier and credentials providers.

Current IDAM Trends

- **Identity & Access Issue**

  User identity and access are not centralized, encouraging lots of security loop holes and threats. Sometimes the user accounts are still in the enable state, when he/she leaves the organization. There is absolutely no control on user access on resources.

- **Dozens of passwords and managing them is a challenge**

  One symptom of the heightened need for security is the growing number of passwords that users must keep track of. Few years ago, most users had only a handful of passwords to remember; a user pretty much had the same password for most systems. Today, casual computer users need a dozen passwords, and sophisticated users need several more. There are cases where the users need to maintain and manage over a hundred passwords.

- **Password theft & other threats**

  Computer users have bigger worries. Password theft plays a less significant role in identity theft than phishing, key logging, viruses, worms and malware, while other malicious software continue to increase. Aspiring thieves who do not have the technical skills to perform attacks themselves can buy malware that others have created. Despite the lack of expertise in security and IdM, users are often the first (and sometimes the only) line of defense against ever more dangerous forms of attack.

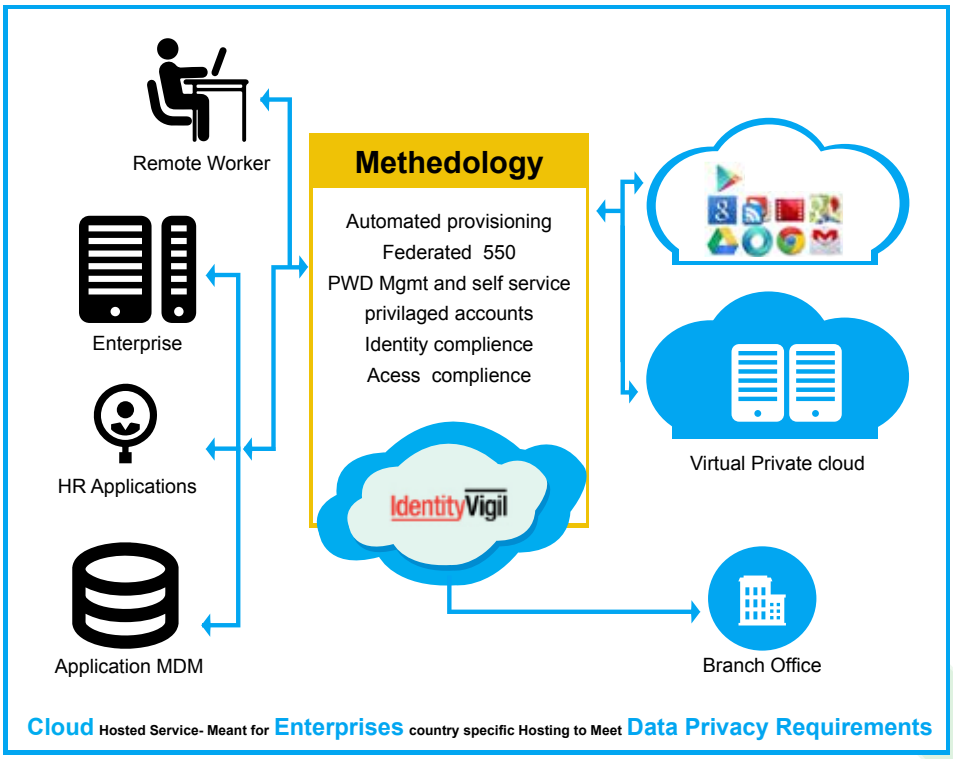
- **Lack of security knowledge**

  Most users find these problems too complex to manage a set of passwords. As a result, many ignore security advice or engage in poor practices such as using simplistic passwords or jotting them down on pieces of papers near their computers. Clearly, an average user lacks the knowledge and skills needed to manage their own security. To resolve this dilemma, a radical shift must take place in IdM research. New directions in IdM research must meet the challenge for improved security by addressing a growing number of threats, while reducing security demands on the user. The centric IAM model proposed in this article provides a potential solution.

A Centric IAM Solution

To design a centric IAM solution, we should consider the below points in mind:

- Centralization of all identity across organization
- Centralization of access across resources/network
- Implement access review process and certify user accesses
- Elimination of multiple credentials
- Elimination of passwords as the primary credential
- Use of advanced security mechanisms such as digital certificates,
- Leverage of mobile devices for centralization
- Deploy & scalable in Cloud as well on-premise infrastructure



Deploy & scalable in Cloud as well on-premise infrastructure

Implementing a user-centric identity & access system with these characteristics would increase both security and usability. This would provide a centralized identity and access across organization. Single credential will eliminate and improve user credential management. Access review half-yearly or yearly will ensure user access across network. Finally, user load would be reduced due to password elimination, single-credential centralization of access and offloading the need for deep technical knowledge to trained security professionals.

Note: IdentityVigil, a Happiest Minds IAM solution has all the above features integrated together.

Conclusion:

Users have dozens of accounts, each accessible through unique passwords of ever increasing complexity, while security threats come from every direction. It is time to change the game. The emergence of personal IdM companies those adopt user centric identity & access management solution in an age of present, generalized mobile devices could set the stage for such a revolution.

About the Author

Sandip Gupta

Experience in areas of IT security (IDAM) Consulting, Designing and Architecture. Nearly 11 + years of IT application development & implementation experience. Working as SME / Architect in the IMSS IAM security practice, HappiestMinds Technologies, Bangalore, India.

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Email: business@happiestminds.com
Visit Us: www.happiestminds.com

Follow us on