IPASJ International Journal of Information Technology (IIJIT)
Web Site: http://www.ipasj.org/IIJIT/IIJIT.htm
A Publisher for Research Motivation ..... Email:editoriijit@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5976

Identity Management Services in the Present IT Era

Aashish Bhardwaj[1], Vikas Kumar[2]

[1]Mewar University, Chittorgarh-312901, Rajasthan, India

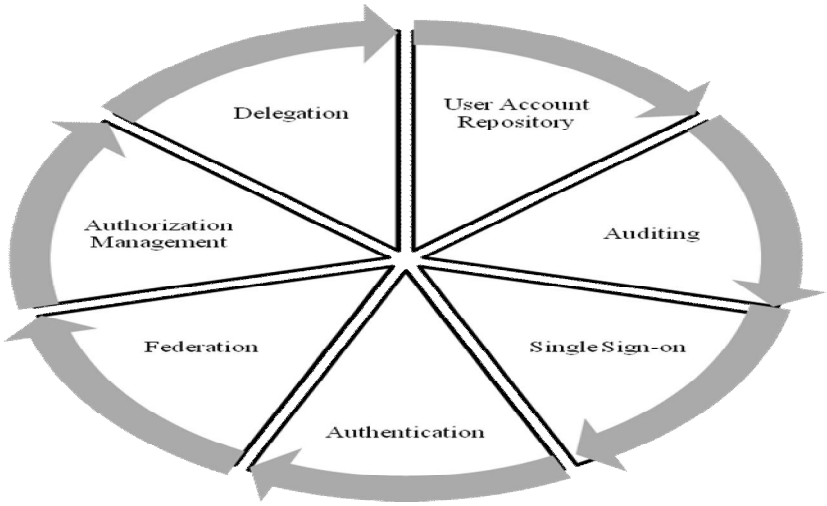
[2] School of Business Studies, Sharda University, Greater Noida, India

ABSTRACT: ***In the present Information technology era, the number of users for mobile, email, debit/credit cards, unique identification numbers is increasing pervasively. This is also bundled with different threats to identity, security, privacy and financial losses. The situation can be improved by use of an effective identity management system which can address these issues in present scenario. This paper defines an identity management system, roles in identity management system and security to prevent different frauds and identity theft incidents. Difference of traditional and modern scope of identity management is presented. A tree of identity management is provided as a requisite for present IT era.***

1. INTRODUCTION

Claub [1] has defined identity management as a tool which uniquely identifies an individual in IT world. An individual may possess several partial identities for interacting with different people and places. Pato & Center [2] has defined a process called identity management which is used for granting access to a person or software agent in a system. Identity Management is considered as a system for maintaining a secure environment with login details. It is a fundamental principle in business relationship, protects privacy and provides regulatory control. Gartner [3] has defined a discipline which allows an individual to access, resources for any correct reasons in a secure manner as identity management.
Different roles of identity management system in an organization are shown in Figure 1.

- **User Account Repository:** There is a centralized repository of accounts with user information. This can be accessed by different systems and thus provide a central control of user accounts.
- **Auditing:** All user accesses are controlled and monitored for security purpose.
- **Single Sign-On:** Identity management enables a technology which allows user to sign-on once in the system. Then all applications are accessed with further authentication.
- **Authentication:** Using data residing in central repository, the system authenticate users for their credentials.
- **Federation:** This includes an external users or group which is provided with delegated user management.
- **Authorization Management:** This is a system by group to manage user access to resources.
- **Delegation:** A user or a group of users delegate a user for associated workflow, review or approval purposes.



Identity management becomes an important tool to understand the risk, whenever any applications are used in incorrect or inappropriate way and results financial as well data losses. Identity Management (IDM) is considered as a superset of all the issues concerned with security in the present IT era [4] – [7]. Thus Identity Management becomes the life cycle maintenance of electronic accounts [8] - [13] and multiple identity management programmes may be necessary in a shared workspace like cloud computing.

Identity Management Life Cycle (as shown in Figure 2) incorporates a synchronization mechanism for identity information and a consistent identity data across multiple service providers. The entire identity lifecycle includes assessing, planning, implementing, auditing, monitoring and maintaining identities & access privileges to the users [14]. Functionally, the Identity Management is divided into two main components i.e. the provisioning components and the administrative components. Provisioning means real time provisioning, this leads to federation of user accounts based on a trusted model. This federation is established at just-in-time the requests are initiated. Provisioning components contains account creation, account updates, role maintenance and account removal. Administrative component is to make sure that Identity Management functionalities are dynamic and easy to deploy in different cloud applications.

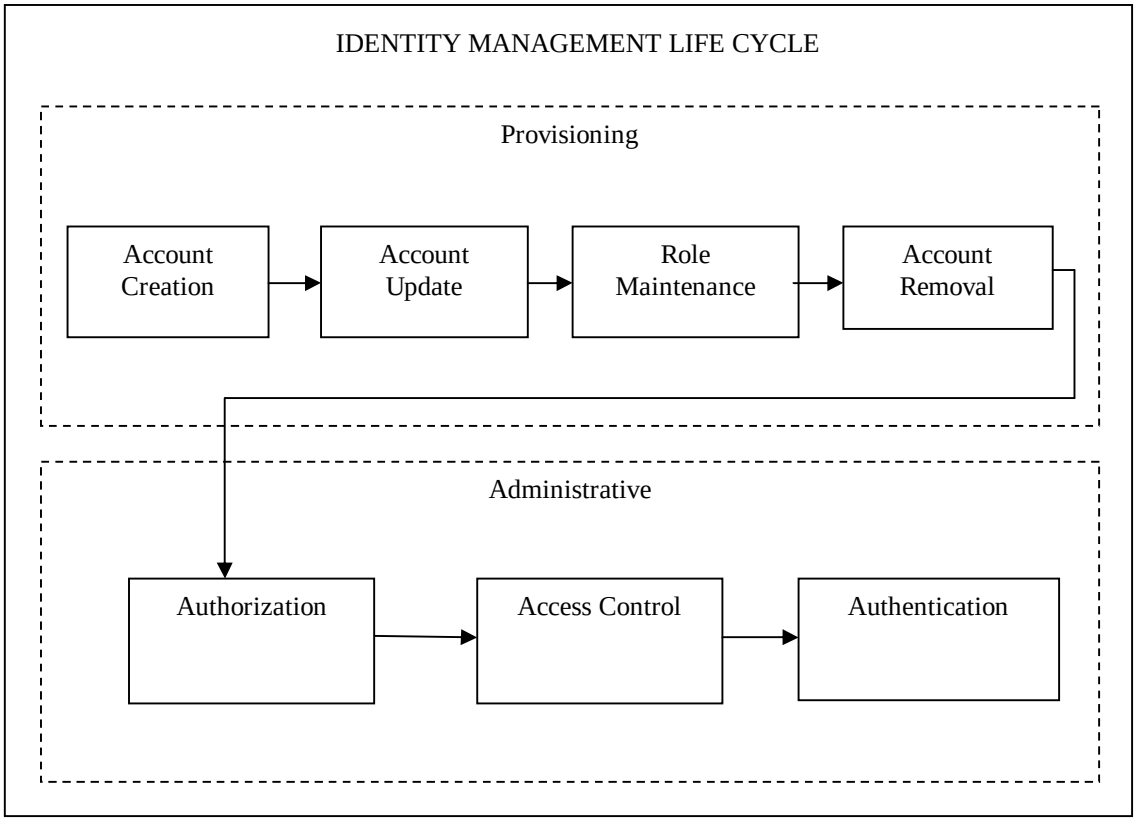


Figure 2: Identity Management Life Cycle

Administrative components contain authentication, authorization and access control. Authentication mechanism is to make one primary user id as a key to authenticate users with multiple service providers. Using this occurrence of multiple identities of the same person with different service providers can be limited.

The authentication component here allows the integration of different authentication mechanisms available such as Light Weight Directory Access Protocol (LDAP), Central Authentication Server (CAS), Windows Live Hotmail Authentication mechanism, OpenID etc. Once the user is authenticated by any authentication mechanism, next all servers trust the user, authorization and access controls are provided. Authorization component provide users the access across multiple service providers and enforce security policies against external threats. Access control provides the user control of their identities and supports multiple and discrete identities to protect user privacy.

Identity information obtained without the consent of concerned person can be used for criminal or unintended activities. Information stolen by online methods includes phishing emails, interception in financial transactions of bank accounts etc lead to information security breaches. For this Rasmusson & Hansson [15] have proposed two approaches to information security i.e. hard and soft security. This can be further illustrated with the following examples:

- In a live performance event, where best performance is judged by viewers who are voting through their mobile phones, the mobile number becomes an identity. There is no check, if a viewer started to vote for the same performer using multiple mobile numbers. It was reported for small screen stars in Mumbai (India), were investigated for purchasing 200 pre-paid SIM cards and distributing the same among their friends to vote for them in the popular reality dance show "*Nach Baliye*"(The Times of India, October 27, 2006) .
- In the electronic marketplace, a seller may hold multiple identities and create confusion to the buyer by interacting with him/her using different identities. Buyer will have no idea that he/she is interacting with the same seller every time.
- last.fm is a social network site where users can recommend music in their groups, colleagues or other persons. A person who is not able to recommend good music to others gain bad reputation. On the other hand, if this user creates a new account in last.fm i.e. a new identity, the reputation starts from scratch and he/she is able to recommend bad music. Listeners may be really bothered with such recommendations and move to other social networks. In this case, the social network is the one which is seriously damaged by losing users [16].

  Many commercially available identity management systems are available like Trew IdM, CA Tech IdM, Courier IdM, eTrust Horacius IdM, Empower IdM, Hitachi IdM, IBM Tivoli, Microsoft Active Directory, Novell IdM, Oracle IdM and Quest IdM.

2. IDENTITY MANAGEMENT AND SECURITY

There are several security challenges for using identity management systems as found by Dhamija and Dusseault [17]. There are many tasks performed by users which make identity management systems vulnerable to security attacks. Such as preference given to identity management system which is available at less cost or bundled free. Easy login and installation of cookies for remembering passwords is preferred by users. Most of the systems are service provider centric instead of user centric. They require user authentication which is sometimes leaking important information through phishing sites. Risk assessment and privacy policy are also not considered in detail which leads to security failure and loss of resources by users.
Users with many security entitlements and unreliable access restriction form a major challenge to identity management. There are many security threats associated with security like spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. There are many frauds and identity theft incidents, some of them are shown in Table 1.

Table 1: Fraud and Identity Theft

S. No.	Agency	Description
1	Federal Reserve (2013)	Unauthorized transactions which took place in 2012 were 31.1 million.
2	Bureau of Justice Statistics (2014)	Identity theft victims in America were 17.6 million in 2014 against 16.6 million victims in 2012.
		42 percent of time Identity theft incidents were involved in stolen Credit Card information in 2014.
		65 percent of time financial losses were experienced for Credit Card frauds in 2016.
3	Bureau of Justice Statistics (2014)	Financial losses were $15.4 billion from Identity theft in 2014 whereas these were $24.7 billion in 2012.

4	Identity Theft Resource Center (2016)	1093 Data breaches took place, among these 13.1 percent were from Credit/Debit card numbers in 2016. Whereas in 2015, 780 Data breaches took place, among these 20.5 percent was from Credit/Debit card numbers.
5	Norman (2016)	Identity theft was 16 percent and 27 percent of US citizens were affected by loss of credit card information in 2016. Whereas in 2015, Identity theft was 15 percent and 22 percent of US citizens were affected by loss of Credit Card information.
6	Total Systems Security (2016)	For security of online purchases consumers preference is 42 percent for credit Card, 26 percent for PayPal, 12 percent for Debit Card, 10 percent for Prepaid or Gift Card and 10 percent had no preference in 2016.

3. TRADITIONAL SCOPE OF IDENTITY MANAGEMENT

Identity management software is mainly used to help users in gaining access of resources in a system, efficiently use them and provide compliance with peripherals [18]. Traditionally the identity management system was expected to provide following;

- A unique user id and password for gaining access in the system. This is bundled with PINs (Personal Identification Number) for financial transactions.
- A system which can handle users list of contact numbers, emails, personal or official addresses and prevent spam or unwanted calls.
- Make use of digital signature to prevent any unwanted access to resources and thefts of identity.

4. MODERN SCOPE OF IDENTITY MANAGEMENT

Tree of Identity Management (Figure 3) has been expanded to provide the modern scope in present IT era. The functionalities include:

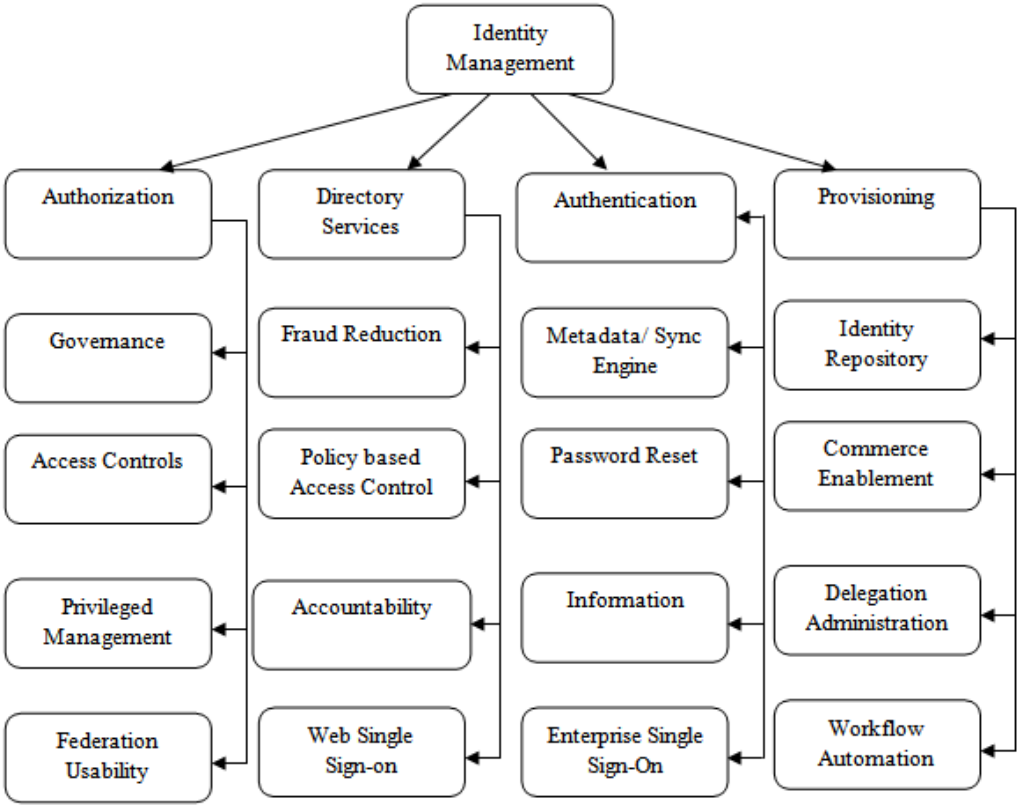


Figure 3: Tree of Identity Management

- Policy for defined access to computer resources.
- Defined rules in cases of identity theft and breaches.
- Access levels to resources in secure manner.
- Up gradation system which can support new services easily.
- Automated workflow from planning, resource allocation, coding and testing phases.
- Quick response to through decentralized system.
- Single password management system for ease of users.

5. CONCLUSION:

Identity Management needs are changing day by day with the growing number of users and increasing risks of security. The software and applications are becoming more and more complex which in turn are also increasing the risks in terms of security and identity. Hence the identity management needs to be seen in a more detailed perspective considering all sub-aspects. So, the identity management definition and tree will help on evading.

REFERENCES

[1] Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. Computer Networks, 37(2), 205-219.
[2] Pato, J., & Center, O. C. (2003). Identity management: Setting context. Hewlett-Packard, Cambridge, MA.
[3] https://gartner.com/doc/reprints?id=1-3F1C5YC&ct=160817&st=sb [29.08.2017]
[4] Huang, H. Y., Wang, B., Liu, X. X., & Xu, J. M. (2010, May). Identity federation broker for service cloud. In Service Sciences (ICSS), 2010 International Conference on (pp. 115-120). IEEE.
[5] Friedewald, M., Vildjiounaite, E., Punie, Y., & Wright, D. (2007). Privacy, identity and security in ambient intelligence: A scenario analysis. Telematics and Informatics, 24(1), 15-29.
[6] Dinoor, S. (2010). Privileged identity management: securing the enterprise. Network Security, 2010(12), 4-6.
[7] Bhardwaj, A., & Kumar, V. (2014). Identity management practices in cloud computing environments. International Journal of Cloud Computing, 3(2), 143-157.
[8] Olsen, T., & Mahler, T. (2007). Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust'–Part II. Computer Law & Security Review, 23(5), 415-426.
[9] Chivers, H., & Clark, J. A. (2004). Smart dust, friend or foe?—Replacing identity with configuration trust. Computer Networks, 46(5), 723-740.
[10] Chen, J., Wu, G., & Ji, Z. (2011). Secure interoperation of identity managements among different circles of trust. Computer Standards & Interfaces, 33(6), 533-540.
[11] Tatli, E. I., & Lucks, S. (2009). Mobile identity management revisited. Electronic Notes in Theoretical Computer Science, 244, 125-137.
[12] Dimitriadis, C. K., & Polemi, D. (2006). An identity management protocol for Internet applications over 3G mobile networks. computers & security, 25(1), 45-51.
[13] Galiero, G., & Giammatteo, G. (2009). Trusting third-party storage providers for holding personal information. A context-based approach to protect identity-related data in untrusted domains. Identity in the Information Society, 2(2), 99-114.
[14] Kumar, V., & Bhardwaj, A. (2018). Identity Management Systems: A Comparative Analysis. International Journal of Strategic Decision Sciences (IJSDS), 9(1), 63-78.
[15] Rasmusson, L., & Jansson, S. (1996, September). Simulated social control for secure Internet commerce. In Proceedings of the 1996 workshop on New security paradigms (pp. 18-25). ACM.
[16] Such, J. M., Espinosa, A., Garcia-Fornes, A., & Botti, V. (2011). Partial identities as a foundation for trust and reputation. Engineering Applications of Artificial Intelligence, 24(7), 1128-1136.
[17] Dhamija, R., & Dusseault, L. (2008). The seven flaws of identity management: Usability and security challenges. IEEE Security & Privacy, 6(2).
[18] Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. Decision support systems, 43(2), 618-644.

Aashish Bhardwaj received his Master of Science in Electronics from Kurukshetra University, Haryana, India and further Masters in Technology in Computer Science and Engineering from the same University. He is a member of Indian National Science Congress Association, Indian Society for Technical Education, Institute of Electronics& Telecommunication Engineers and Computer Society of India and has contributed many research papers to reputed journals and conferences. Presently, he is

working for PhD degree in Computer Science & Engineering from Mewar University, Chittorgarh, India.

Vikas Kumar received M.Sc. in Electronics from Kurukshetra University, Haryana, India. This was followed by M.Sc. in Computer Science and further Ph. D. from the same university. His Ph.D. work was in collaboration with CEERI, Pilani and he has worked in a number of ISRO sponsored projects. Dr. Kumar has designed and conducted number of training programs for the corporate sector and has served as a trainer for a number of Government of India departments. Along with six books, he has more than 100 research papers to his credit in various national and international conferences and journals. He was the Editor of International Quarterly Refereed Journal "Asia-Pacific Business Review" during June 2007-June 2009. He is a regular reviewer for a number of international journals and prestigious conferences. Presently, He is a Professor at the Sharda University, Greater Noida and a visiting Professor at the Indian Institute of Management, Indore.