iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** II **Month of publication:** February 2024

DOI: https://doi.org/10.22214/ijraset.2024.58386

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue II Feb 2024- Available at www.ijraset.com

Identity and Access Management: Concept, Challenges, Solutions A Small Snapshot Review

Dr. Vivek Ramakrishnan, Dr. Pete Dnyandeo Jageshwar
[1]*Assistant Professor, Electronics and Telecommunication Department, Atharva College of Engineering, Malad, Mumbai*
[2]*Professor & HOD, Electronics and Telecommunication Department, Datta Meghe College of Engineering, Airoli, Navi-Mumbai*

Abstract: ***Modern society recognizes the significance of Identity and Access Management. It's the method through which information is controlled in terms of who gets access to what and when. Creation of user and system identities is an IAM activity. Data and information sharing relies heavily on safe user access. In addition, most businesses are realizing the growing value of electronic data. Strong authentication is a common solution to this problem and is becoming more and more necessary as the standards for access protection rise. The two most critical IAM concepts that must be handled by the business are identity and access. More and more businesses are turning to an automated system to handle these tasks. But it opens up a new danger. Since these technologies lack the wit to make judgements on their own, we must supplement them with our own brainpower employing a variety of data mining algorithms. This allows us to save data for later model building. Everything you need to know about the difficulties of Identity and Access Management may be found in this document. A potential answer is provided for these problems.***

Keywords: Access, Authentication, Data Mining, Automated, Electronic.

I. INTRODUCTION

Companies now not only need to connect and provide a variety of information systems, but they are also more concerned with complicated value chains. This is causing a blurring of distinctions between service providers, customers, and rivals. Consequently, businesses must have nimble and adaptable procedures for exchanging data and information electronically. Effective identity and access management systems are essential for such operations. IAM is the procedure through which the timing and scope of data access is controlled. Creation of user and system identities is an IAM activity. Management of Identities and Privileges The emergence of I am as a vital basis for realizing the cost savings, managerial control, operational efficiency, and most significantly, company development potential of ecommerce is a relatively new phenomenon. Organizations must control user access to data and programmed that may reside on any number of internal or external computer networks. For a rising number of identities inside and outside the organization, they must do so without jeopardizing security or disclosing confidential information, which is even more crucial. The term "IAM" refers to the people, procedures, and products used to control who has access to what inside an organization. A system for managing digital identities and access privileges is called an identity access management (IAM) system. The framework comes with every tool required for identity management. IAM technology may be used to automate initiating, collecting, recording, and managing user identities and the related access entitlements. This guarantees that all users and services are verified, authorized, and audited in accordance with a unified understanding of security policy. 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 business needs to ensure data accuracy for the IAM Framework to function effectively. Authentication, authorization, user management, and a centralized user repository are the four fundamental elements of IAM (Enterprise Directory). The main goal of IAM Framework is to make sure that the appropriate people have access to the right resources at the right times.

II. AUTHENTICATION

In this context, the terms "authentication management" and "session management" are interchangeable. When a user first interacts with an application system or a resource, they must go through the authentication process. When a user interacts with an application system after authenticating, a session is created and utilized as a point of reference throughout that interaction until the user logs out or the session is canceled in some manner (for example, by a timeout). When the user ID / password technique is used, a password service module is often packaged along with the authentication module. A user no longer has to log in each time they go between apps or systems that are all controlled by the same Identity and Access Management (IAM) Framework thanks to the Single Sign-On service provided by the authentication module.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue II Feb 2024- Available at www.ijraset.com

III. AUTHORIZATION

The module responsible for deciding whether a user has access to a given resource is called "authorization." The URL being used to request this resource is checked with the authorization rules held in an Identity and Access Management policy store in order to establish whether or not a user is authorized to access it. An important part of role-based access control is the authorization module. Furthermore, the authorization model may provide intricate restrictions for entry depending on a wide range of factors, such as data, information, or regulations, such as user characteristics, user roles / groups, actions conducted, access channels, time, resources sought, external data, and business rules.

See below diagram

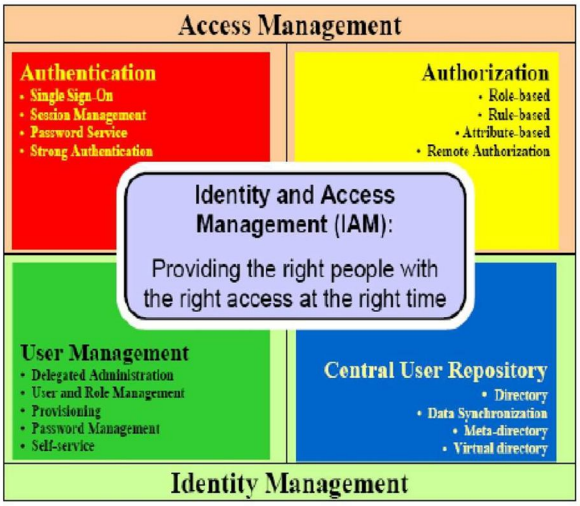


Fig.1.1: What is Identity Management

IV. USER MANAGEMENT

User management includes provisioning of users and groups, password management, and administration of roles and groups. A user's identity and permissions are managed by a system, and this is what the term "user management module" refers to. A technological component called user life cycle management enables a corporation to manage a user account's whole lifespan, from provisioning through de- provisioning. There should be some centralized user administration, while some tasks should be given to individual users. In a delegated administration model, work is given straight to the user departments inside an organization. Another method of delegation that may improve the accuracy of system data is to provide the responsibility of updating to those who are most familiar with the situation and the information. The notion of self-service is also important to user management. An organization may save time and effort on identity management thanks to the self- profile management solution. Another popular self-service tool that relieves the help desk staff's work is self-password reset. Integrated workflow capabilities is crucial for user management since certain user actions, such as the providing and de- provisioning of user accounts, need administrator approval.

V. CENTRAL USER REPOSITORY

The centralized user repository not only verifies client credentials but also stores and distributes user identification data to other services. The Central User Repository provides a holistic, or logical, perspective on the identities inside an organization. Central User Repository has mostly shifted towards using directory services that adhere to LDAPv3 specifications. Meta-directory and Virtual directory are both useful for managing user identities stored in various systems and applications. A meta-directory is a database that combines information from several directories into a single master directory. In most cases, it also includes a service for bidirectional data synchronization with other identity providers". To provide a consistent LDAP display of aggregated identifying information, many databases storing various groups of users are merged in real time behind the scenes.

VI. NEED OF IAM

Data and information sharing relies heavily on secure user access. In addition, most businesses are realizing the growing value of electronic data. Strong authentication is a common solution to this problem and is becoming more and more necessary as the standards for access protection rise.

Today's IAM tools make it easy to manage people and their permissions in a variety of ways, opening up new possibilities for teamwork. In addition, IAM is necessary for the usage of cloud services since they may include the outsourcing of data, which necessitates the precise definition and monitoring of data handling and access. Companies must also deal with the complexity of IAM data in its many formats, since it is often given by legacy systems. In order to meet current security requirements and act quickly if required, they must locate and combine these data sources and build a data lifecycle. As seen in the figure on the right, IAM duties may be roughly classified into three tiers. The compliance and review processes are also defined by the governance level. Identity, access, and authorization tokens may all be managed at the management layer. Information is reviewed and synchronized in real time at the execution level.

Because IAM initiatives don't immediately boost profits or provide new features, they might have trouble being funded. However, serious threats to compliance and even the security of an organization may result from inefficient identity and access management. These management flaws make it more likely that harm will be done, from both internal and outside influences.

It has always been the responsibility of the administration to ensure that the necessary flow of business data is maintained while also limiting access to it. Recent disruptive advances, such as bring your own device (BYOD), cloud computing, mobile apps, and a more flexible workforce, have further compounded an already challenging enterprise IT environment. Access control is becoming more complex as the number of devices and services that need to be monitored grows. It gets increasingly challenging to manage identification and access when individuals move between jobs within an organization. When an employee's responsibilities change, they are often given additional permissions, but those aren't always removed when they're no longer needed. Privilege creep is the gradual escalation of privileges as a consequence of circumstances and requests, such as having access to resources normally reserved for employees, as opposed to explicit access requests. There are two ways in which privilege creep might compromise security. An overprivileged worker has the chance to access sensitive data and programmed without authorization. In addition, if a malicious actor compromises a user account with elevated rights, he may immediately obtain access to other resources. Both have the potential to compromise private data.

This accumulated privilege usually serves neither the employee nor the company very well. A possible benefit might arise if the worker is ever requested to perform unanticipated responsibilities. However, if an attacker compromises a highly privileged employee account, they may find their task considerably simpler. The retention of access rights after termination of employment is another common result of insufficient attention to identity access management.

VII. CONCEPT OF IDENTITY AND ACCESS MANAGEMENT

A. *Definition of Key concept*

1) *Identity:* Identity refers to the property or properties that define an individual or a machine in a certain way. Any combination of what you know, such as a password, and what you have, such as other pieces of personal information, may be used to get access.
2) *Access:* The data evidencing the privileges associated with the identity in question. Users may be given varying degrees of access to this data in order to carry out a variety of transactional tasks. Transactional operations include copying, transferring, adding, modifying, deleting, reviewing, approving, and cancelling.
3) *Entitlements:* Entitlements refer to the set of permissions that allow one to carry out a certain kind of transaction. Access rights are also referred to as entitlements. The who, what, where, when, and why of information technology is identity and access management. These are only a few of the many different technologies and security practices that are included. Others include secure single sign-on (SSO), user provisioning and deprovisioning, authentication, and authorization. Fortune 2000 organizations and governments all over the world have come to rely on a strong IAM platform as the cornerstone of their GRC strategy over the course of the past several years. The statistics support this claim: We estimate that the necessity to achieve regulatory compliance regulations accounted for around 80% of the over $4 billion in license and maintenance fees generated by the IAM industry in 2010.

This lays the foundation for the company's larger GRC infrastructure, an area in which SAP, NetIQ, and Novell have accumulated years of experience and knowledge. According to IDC, GRC infrastructure is made up of IT-based solutions for things like policy and procedure creation, documentation, enforcement and operationalization, as well as monitoring, testing, and verification of controls. It's a continuous, ever- changing procedure. There is a larger need than ever before for robust security and GRC practices as more businesses decentralize with branch and home offices, remote staff, and the consumerization of IT.

B. Function Of Identity Management

The identity management system is a database that records data pertaining to the whole identity management setup. Authorization, authentication, user registration and enrollment, password management, auditing, user self-service, centralized administration, and delegated administration are all provided based on this data.

1) *Stores Information:* Databases (such as Oracle, DB2, MS SQL Server), applications (such as business, Web, and desktop applications), devices (such as cell phones, pagers, and card keys), facilities (such as warehouses, office buildings, conference rooms), groups (such as departments, workgroups), operating systems (such as Windows, Unix, MVS), people (such as employees, contractors, and customers), policies (such as security policy, access control policy), and roles (such as titles, responsibilities, and job functions) are among the resources that the identity management system holds information about.
2) *Authentication and Authorization:* Users, both internal and external, may now be verified and granted appropriate access thanks to the identity management system. Identity management systems require users to provide credentials such as a username and password, digital certificate, smart card, or biometric data whenever they make a request to access a resource. Following successful authentication, the identity management system grants the user the level of access that is commensurate with their identity and other criteria. By having the access control component handle future authentication and authorization requests, the user will have fewer passwords to keep track of and fewer occasions to go through the login process. That's what we mean when we talk about "single sign-on" or "reduced sign-on." While providing single sign-on for all corporate apps is an ideal, it is presently unfeasible objective for an identity management system to provide single sign-on for all Web applications.
3) *External user Registration and Enrolment:* External users may create accounts in the identity management system and enroll for access rights to a specific resource. The user will be given the option to create an account if they are unable to authenticate with the identity management system. After signing up for an account and proving their identity, users must enroll to have access to the materials they require. The resource owner may either automatically authorize enrollment based on predetermined rules or review each enrollment individually. Access to the resource is allowed only once the user has enrolled in and been verified by the identity management system.
4) *Internal user Enrolment:* In order to get access to restricted areas, workers might register with the identity management system. Because they already have an identity inside the identity management system, internal users will not be offered the opportunity to register, unlike external users. Internal users follow the same steps as external users to enroll.
5) *Auditing:* Information about users and their permissions may be audited more easily with the help of an identity management system. Users' permissions may be checked using the identity management system. In order to provide auditors with reliable information about users and their permissions, the identity management system gathers data from reliable sources.
6) *Central Administration:* Administrators are afforded the convenience of a consolidated identity management system. Both the identity management system's content and its architecture may be centrally managed by administrators.

C. An Increasingly Distributed Workforce

A flexible work environment and the elimination of geographical restrictions are two ways in which businesses may attract and retain top personnel. The ability to have workers operate outside of the typical office space has several advantages for both employers and staff members. Enterprise IT teams confront a considerably more formidable problem, however, when dealing with workers located all over the nation or perhaps the world: providing a uniform experience for employees accessing to corporate resources without compromising safety. As mobile technology advances, IT departments lose oversight and control over how their staff completes tasks. The answer is an enterprise-wide, centralized IAM solution that gives IT teams full visibility and control over their scattered workforces once again.

D. Distributed Applications

Users can access vital business software like Salesforce, Office 365, Concur, and more through any web-enabled device, anytime, anywhere, thanks to the proliferation of cloud computing and SaaS. But as the number of distributed apps grows, so does the difficulty of controlling access to them through individual user identities.

Users have a hard time keeping track of several login credentials for each programme, and IT is hit with escalating support expenses as a result of users' growing dissatisfaction. Whether the mission-critical applications are housed in conventional data centers, private clouds, public clouds, or a hybrid mix of various locations, a comprehensive IAM solution can assist administrators consolidate, regulate, and simplify access rights.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue II Feb 2024- Available at www.ijraset.com

E. Productive Provisioning

IT staff must manually supply user accounts without a centralized IAM system. When employees have to wait longer than necessary to access critical business systems, they are less productive. However, there might be major security issues if former workers or those who have been moved to other departments do not have their access privileges revoked. IT workers need to remove access to company data as soon as possible to prevent this security breach. This forces IT departments in many businesses to manually remove access by going through user accounts and learning what resources each user has been granted access to. Provisioning and revoking access manually is time-consuming, error-prone, and may easily be overlooked. Managing user identities and permissions in this manner is neither efficient nor sustainable, especially for big organizations. By using a comprehensive IAM solution, IT can finally exert complete control over the permissions granted to workers, partners, contractors, suppliers, and visitors. Strong security measures may be enforced more quickly and with fewer opportunities for human mistake thanks to automated provisioning and de provisioning.

F. Bring Your Own Device (BYOD)

In today's organizations, there is really no option except to manage or not manage. Individuals in the organization (employees, contractors, partners, etc.) are increasingly using their own devices to access the company's internal network. The difficulty with BYOD is not whether personal devices will be connected to the company's network, but rather whether IT will be able to respond fast enough to protect corporate data and prevent loss of productivity without limiting workers' choices. Almost all businesses now have a Bring Your Own Device (BYOD) policy that allows employees to use their own encrypted devices to access corporate data. However, compared to a networked laptop or desktop workstation, using a mobile device to access internal and SaaS apps might be a tedious process. Furthermore, IT workers may find it difficult to control which devices and users have access to sensitive company information. The solution is for businesses to have a plan that makes it simple and safe to provide and revoke access to corporate apps on personal and company-owned mobile devices in accordance with internal policies and legal requirements. Additionally, IT departments must implement solutions that can grow to handle the flood of devices seeking to burden the business network in light of technological advancements such as the move towards an Internet of Things.

G. Password Problems

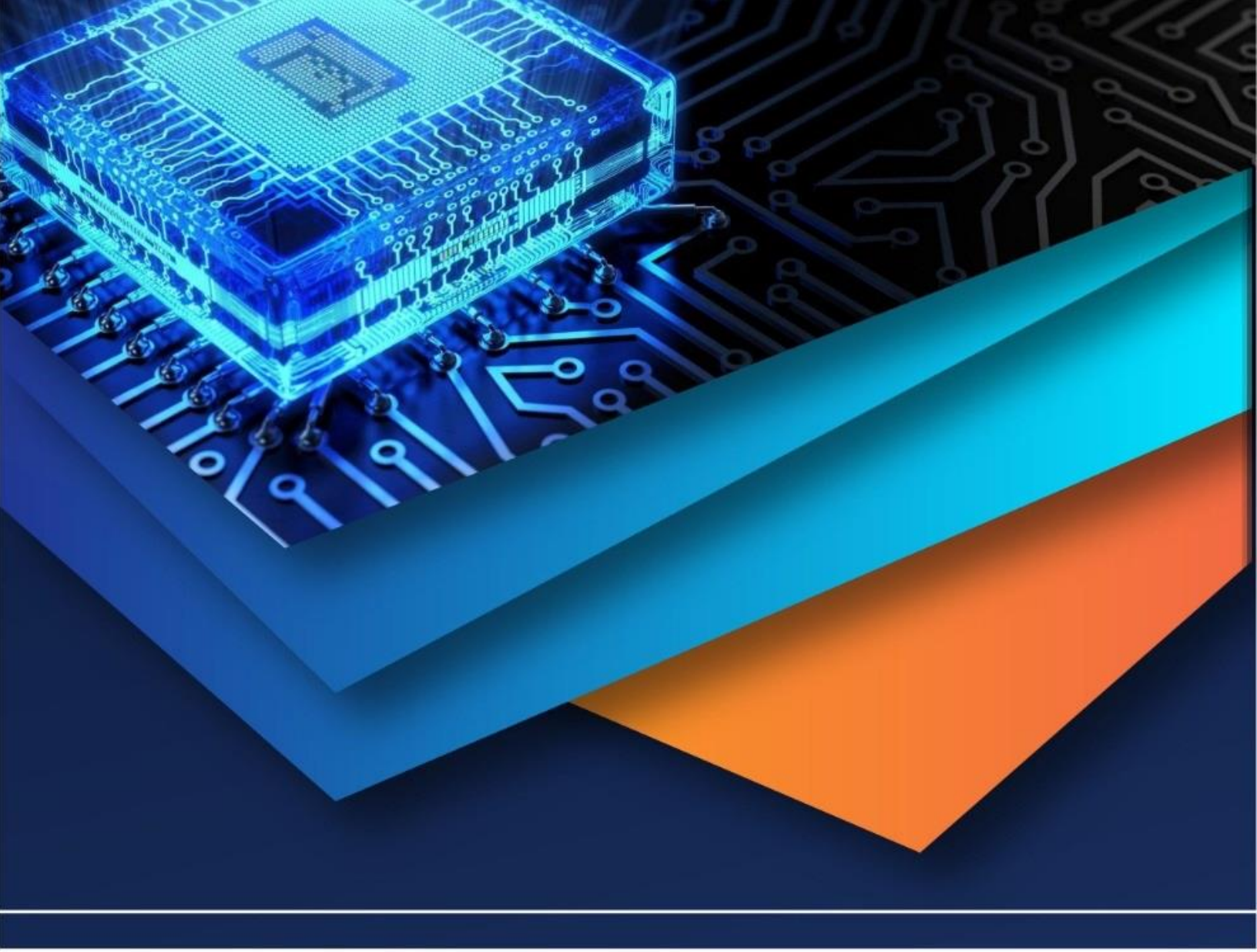
As the number of cloud-based apps continues to rise, it becomes more difficult for workers to keep track of the many credentials they need to access them. Employees may get frustrated as they are forced to spend more time than necessary monitoring password lists, which may need to be updated as often as once every 30 days for some apps. In addition, when workers have password issues, they often contact IT for assistance, which may rapidly and frequently deplete precious resources. Fortunately, by extending secure single sign-on (SSO) capabilities to SaaS, cloud-based, web-based, and virtual applications via the use of federated user identification, enterprises may effectively eliminate password concerns. To simplify authentication and attribute sharing across many domains, SSO may centralize password management. Industry Data Security Standards (PCI DSS) are just some of the regulations that may be supported by a solid IAM system. In example, a technology that automates audit reporting may facilitate regulatory conformity by streamlining operations

VIII. CONCLUSION AND FUTURE WORK

When it comes to managing identities, it's crucial to prioritize effectiveness, safety, and compliance. Despite the obvious positive effects of deploying a robust IAM solution, the process of doing so may be disruptive even to the best-intentioned of businesses. But when businesses factor in the price of a security breach or examine the inefficiencies inherent to manually providing and de-provisioning access to corporate resources, the need becomes obvious: However It is time for the federal government to form an IAM team capable of creating and enforcing rules for managing identities throughout the whole government. Traditional security perimeters are decreasing in size. The reality of a mobile workforce and a complex, decentralized application network are important considerations for businesses looking for IAM solutions. Reduced expenses, less demands on IT, and more complete data to aid in compliance with regulatory requirements are just a few of the benefits that may accrue from implementing an effective IAM system. In addition, businesses may guarantee safety by introducing solutions with robust authentication and authorization, and users' frustrations can be alleviated via the provision of frictionless access to cloud-based apps through Single sign on. The capacity to develop rules based on contextual and granular data will also grow in significance as the complexity of identity and access management increases. Businesses will benefit from IAM systems that enable rapid distribution of access to workers, partners, and contractors by collecting and making choices based on user identification, device, location, and the requested resource. 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
[12] https://en.wikipedia.org/wiki/Identity_management
[13] http://searchsecurity.techtarget.com/definition/identity-access- management-IAM-system.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY