iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XI **Month of publication:** November 2021

DOI: https://doi.org/10.22214/ijraset.2021.39029

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: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

Identity Access Management (IAM), Privilege Access Management (PAM) & Security Operation Center (SOC)

Hardik Varma
Rashtriya Raksha University, India

I. INTRODUCTION

Cloud computing is a nascent and rapidly evolving model, with new aspects and capabilities being added regularly by researchers around the world. Cloud computing has its roots in large-scale distributed computing technology. It is in fact an extension of grid computing, distributed computing, and parallel computing are the emerging future technology which will simply plug in to cloud for the computing resources they need.

In Security-as-a-service model the focus is on security delivered as cloud services;

i.e. security provided through the cloud instead of on premise security solutions. Identity and Access Management (IAM), Privilege and Access Management (PAM) focuses on authentication, authorization, administration, secure access, Zero Trust Priviledge of Identities and audits. Its primary concern is verification of identity of entity and grating correct level of access for resources which are protected in the cloud environment. dentity Management is the foundation for "real" digital transformation; the secure, flexible and adaptive IT infrastructure that every company, government agency and institute of higher education strives to achieve.

The establishment of identities and distribution of those identities will be leveraged by virtually every substantive application and process throughout most organizations. Identity should ultimately be a "utility"; it should be easy to identify individuals, applications and things and use them as needed under proper security controls that are privacy-centric. The management of identities is also a critical part of how organizations directly interact with consumers and trading partners. The IAM & PAM implemented as the cloud service can benefit the user with all the advantages offered by Security-as-a-service. I have implemented a proof-of-concept (POC) of SaaS. The relevant standards and technologies are also implemented & discussed for providing secure access to cloud users.

In this report, I propose the Identity and Access Management (IAM), Privilege and Access Management (PAM) as a service framework, Tools/Technology and Implementation.

II. LITERATURE REVIEW

Overview of IAM, PAM functions and tools

A. Key Trends and Technology Trends

To give the future of Identity Management the right context, we must take a quick look at some of the key trends that will drive Internet and information technology over the next five years. Most of these trends are not new; they represent existing trends we expect to continue to be relevant over the next several years. These trends will directly impact the next generation of identity management products and services. Key trends include:

1) *Internet of Things (IoT):* The Internet is extending its web to include almost anything one can think of: from light bulbs to cars and refrigerators to traffic lights, to sensors monitoring our movements and medical devices. IoT will be pervasive in business with real time monitoring and sensors coupled with advanced workflow technologies providing greater efficiencies and responsiveness. Almost everything in the physical world can be tagged, accessed, analyzed, connected and, in theory, optimized. These devices can be connected to the Internet and to other individuals and organizations, but there are complex relationships to manage, personal information to protect and a plethora of challenging security concerns. Establishing identities for these items and enabling appropriate access for these identities throughout the connected ecosystem is stretching identity to new limits.

2) *Everything Moving to the Cloud:* Cloud computing will continue to gain momentum and is the primary means of delivering applications and services to consumers and among businesses. Identities are being stored in the cloud and identity services are increasingly cloud-based. Cloud-based applications will also store identity information and will authenticate users. Cloud-based services are also supporting the movement to DevOps and microservices. Wireless and Mobile. Wireless access is increasingly an expectation in most parts of the world and is shaping the applications for both businesses and individuals. Access via mobile devices is becoming the first choice as intelligent phones, tablets and appliances proliferate. The advent of mobile has major ramifications for both identity management and security. These trends will accelerate over the next five years with smarter and more powerful mobile devices.
3) *Bring Your Own Device (BYOD):* More and more employees are using their own personal devices rather than corporate-delivered systems to access company business and Internet-based applications and services. BYOD, wireless and mobile means that identification based on static location or a corporate device is no longer a given.
4) *Artificial Intelligence (AI) and Machine Learning (ML):* From machine learning to natural language processing, artificial intelligence and cognitive computing are elevating beyond speech recognition and rules-based systems to help organizations consume and derive value from big data and drive decision-making through powerful analytics.
5) *Security Investment, Visibility and Intelligence:* Given the increasing numbers of breaches, accessibility to personal data, sophistication of cyber-criminals and corporate risk aversion, security and risk programs are given higher and higher priorities in organizations and for individuals. This acceleration has occurred over the past several years and we expect it to continue to accelerate for the foreseeable future. As the perceived importance of security increases, there will be corporate organizational changes with CISOs reporting to CEOs or Boards instead of CIOs.
6) *DevOps and Microservices:* Many organizations are moving from the traditional monolithic approach to application development to more "Netflix" like DevOps and Microservices models in which applications are broken down into the most basic services and developers are responsible for not just the development, but also the operational support. This type of model is highly scalable and drives more continuous integration and delivery than the monolithic application model that has existed for much of the past 40 years. The goal is to provide updates on a daily or weekly basis (as needed) as opposed to waiting for annual (or worse) release cycles.
7) *Blockchain:* The underlying technology developed to support Bitcoin has grown like wildfire in the past three years and is continuing to accelerate. At its core, Blockchain provides a transaction record that doesn't require a central third party to mediate is tremendously disruptive and has inherent security capabilities as part of its foundation.

III. IDENTITY MANAGEMENT; IDENTITY AS A UTILITY

The Future of Identity Management; Identity as a Utility Identity Management needs to become an "Identity Utility". Much like electricity and water in most modern cities; when you need or want it, the service is there…and it is simple, ubiquitous, and safe to use…like turning a faucet or plugging in an appliance.

A simple and frictionless experience for the developer, employee, customer or administrator will be critical for the next generation of identity services.

Identity as a Utility (IaaU) starts with a reliable and consistent means of collecting, organizing and disseminating data. Since enterprise data generally lives in a multitude of disparate silos, the sharing of data and the orchestration of the changes to the data across these silos has been the traditional cornerstone of many solutions and its roots can be seen in current IAM challenges such as user account provisioning.

Event triggers, such as changes to authoritative sources of data like Human Resource Management Systems (HRMS), result in the automatic creation of user accounts, assignment of access privileges, and the propagation of user attributes for as many downstream target environments as can exist in an organization. Identity abstraction can be thought of as the ultimate services–oriented IAM architecture.

The target is a ubiquitous service that provides identity data to people, applications and network services. The future of Identity Management will be built on a flexible and highly accessible foundation that integrates data from many environments and provides secure access for many identity consumers. The challenge in getting to the "utility" state is that most enterprises have so many environments and processes to be normalized and integrated in some cohesive way. This is in part due to a lack of standardization of both integration capabilities and of processes and procedures.

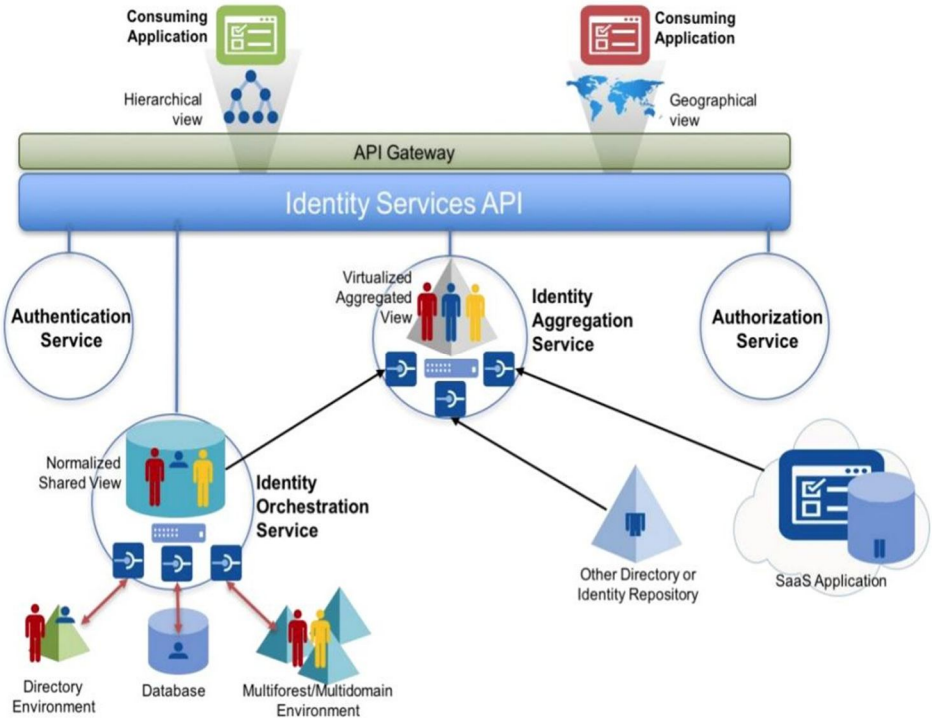
IV. KEY PRIVILEGED ACCESS MANAGEMENT CHALLENGES

Organizations face a number of challenges protecting, controlling and monitoring privileged access including:

1) *Managing account credentials:* Many IT organizations rely on manually intensive, error-prone administrative processes to rotate and update privileged credentials. This can be an inefficient and costly approach.
2) *Tracking Privileged Activity:* Many enterprises cannot centrally monitor and control privileged sessions, exposing the business to cybersecurity threats and compliance violations.
3) *Monitoring and Analyzing Threats:* Many organizations lack comprehensive threat analysis tools and are unable to proactively identify suspicious activities and remediate security incidents.
4) *Controlling Privileged User Access:* Organizations often struggle to effectively control privileged user access to cloud platforms (Infrastructure as a Service and Platform as a Service), Software as a Service (SaaS) applications, social media and more, creating compliance risks and operational complexity.
5) *Protecting Windows Domain Controllers:* Cyber attackers can exploit vulnerabilities in the Kerberos authentication protocol to impersonate authorized users and gain access to critical IT resources and confidential data.

A. Working Of Identity Services

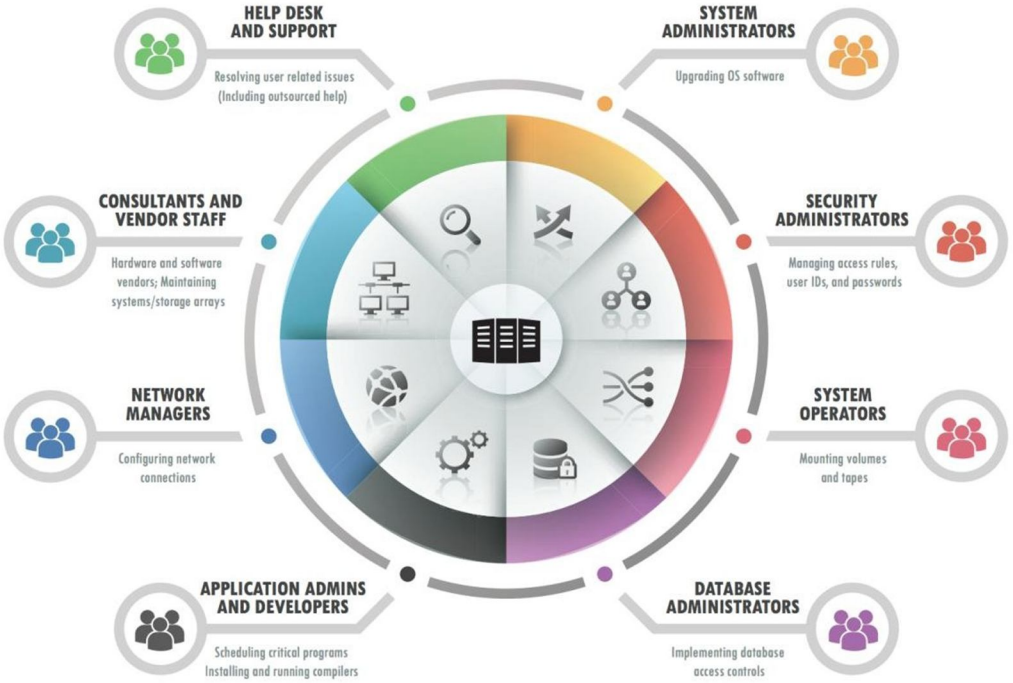
Identity Services may be implemented in an organization in the service of consuming applications.



Example of Identity Services

In this diagram, two different applications are consuming the same identity information, but each get the view of this information that best suits their respective needs. They access this data through the identity services API which abstracts the details of the underlying authentication service, authorization service, identity orchestration service and identity aggregation service. The identity orchestration service assembles and normalizes the identity information that is shared amongst the underlying directory, database and multiforest environments. The identity aggregation service then takes this normalized shared view of the data and aggregates it with data collected from other sources to create a dynamically generated virtualized view for each application in the format that they requested. This how Identity as a solution works.

B. Essensial of Priviledge Access Mamagement



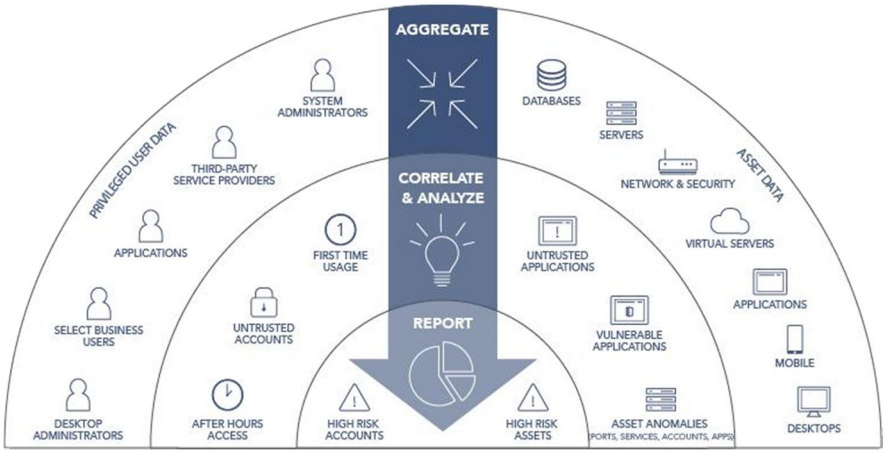
V. PRIVILEGED ACCESS MANAGEMENT PRACTICES

The more mature and holistic your privilege security policies and enforcement, the better you will be able to prevent and react to insider and external threats, while also meeting compliance mandates.

Here is an overview of the nine most important PAM best practices:

1) *Establish and Enforce A Comprehensive Privilege Management Policy:* The policy should govern how privileged access and accounts are provisioned/de-provisioned; address the inventory and classification of privileged identities and accounts; and enforce best practices for security and management.
2) *Identify and Bring Under Management All Privileged Accounts and Credentials:* This should include all user and local accounts; application and service accounts database accounts; cloud and social media accounts; SSH keys; default and hard-coded passwords; and other privileged credentials – including those used by third parties/vendors. Discovery should also include platforms (e.g., Windows, Unix, Linux, Cloud, on-prem, etc.), directories, hardware devices, applications, services / daemons, firewalls, routers, etc. The privilege discovery process should illuminate where and how privileged passwords are being used, and help reveal security blind spots and malpractice, such as: SSH keys reused across multiple servers
3) *Enforce Least Privilege over end Users, Endpoints, Accounts, Applications, Services, Systems, etc:* A key piece of a successful least privilege implementation involves wholesale elimination of privileges everywhere they exist across your environment. Then, apply rules-based technology to elevate privileges as needed to perform specific actions, revoking privileges upon completion of the privileged activity.
4) *Enforce Separation of Privileges and Separation of Duties:* Privilege separation measures include separating administrative account functions from standard account requirements, separating auditing/logging capabilities within the administrative accounts, and separating system functions (e.g., read, edit, write, execute, etc.). When least privilege and separation of privilege are in place, you can enforce separation of duties. Each privileged account should have privileges finely tuned to perform only a distinct set of tasks, with little overlap between various accounts.
5) *Segment Systems and Networks:* To broadly separate users and processes based on different levels of trust, needs, and privilege sets. Systems and networks requiring higher trust levels should implement more robust security controls. The more segmentation of networks and systems, the easier it is to contain any potential breach from spreading beyond its own segment.

6) *Enforce Password Security best Practices:* Centralize security and management of all credentials (e.g., privileged account passwords, SSH keys, application passwords, etc.) in a tamper-proof safe. Implement a workflow whereby privileged credentials can only be checked out until an authorized activity is completed, after which time the password is checked back in and privileged access is revoked.Ensure robust passwords that can resist common attack types (e.g., brute force, dictionary-based, etc.) by enforcing strong password creation parameters, such as password complexity, uniqueness, etc. Routinely rotate (change) passwords, decreasing the intervals of change in proportion to the password's sensitivity. A top priority should be identifying and quickly changing any default credentials, as these present an out-sized risk. For the most sensitive privileged access and accounts, implement one-time passwords (OTPs), which immediately expire after a single use. While frequent password rotation helps prevent many types of password re-use attacks, OTP passwords can eliminate this threat. Eliminate password sharing—each account should have a unique login to ensure a clear oversight and a clean audit trail. Never reveal passwords—implement single sign-on (SSO) authentication to cloak passwords from both users and processes.
7) *Monitor and Audit all Privileged Activity:* This can be accomplished through user IDs as well as auditing and other tools. Implement privileged session management and monitoring (PSM) to detect suspicious activities and efficiently investigate risky privileged sessions in a timely manner. Privileged session management involves monitoring, recording, and controlling privileged sessions. Auditing activities should include capturing keystrokes and screens (allowing for live view and playback). PSM should cover the period of time during which elevated privileges/privileged access is granted to an account, service, or process.
8) *Enforce Vulnerability-based least-privilege Access:* Apply real-time vulnerability and threat data about a user or an asset to enable dynamic risk-based access decisions. For instance, this capability can allow you to automatically restrict privileges and prevent unsafe operations when a known threat or potential compromise exists for the user, asset, or system.
9) *Implement Privileged threat/user Analytics:* Establish baselines for privileged user activities and privileged access, and monitor and alert to any deviations that meet a defined risk threshold. Also incorporate other risk data for a more three-dimensional view of privilege risks. Accumulating as much data as possible is not necessarily the answer. What is most important is that you have the data you need in a form that allows you to make prompt, precise decisions to steer your organization to optimal cyber security outcomes.



Privileged threat analytics: aggregating

VI. PROBLEMS IDENTIFIED & IMPLEMENTATION METHODOLOGY

The lack of visibility and awareness of privileged users, accounts and credentials makes it difficult for organizations to detect malicious use of these— harmful activities can go on for an extended period without recognition. These accounts can add up and become long forgotten, providing dangerous backdoor access for attackers. While most organizations consider a "hacker" to be an external threat, in many instances it could be an inside job. Former or current employees that may have uncontrolled access to privileged accounts may also be a threat—benefitting from the internal knowledge of where protected assets and information are and how to get to them.

In terms of compliance, fines can be levied against your company for being associated with data exposure. Privacy regulations, including GDPR and CCPA, require that organizations ensure proper security protocols and data stewardship.

Privilege in IT is like oil: The machine cannot run without it, but too much and there will be a mess. The industry has struggled with privilege over the years and, with the proliferation of hybrid multi-cloud computing environments, it must improve privileged access management (PAM). The key requirements to improve PAM are:

1) Better PAM integration with identity governance and administration (IGA).
2) Support for just-in-time (JIT) access.
3) Integration with DevOps pipelines and service accounts.

The vast majority of organizations today rely heavily on technology and IT software to manage business operations. This means that, across industries, taking the proper steps to secure your IT environment is of critical importance. Identity and access management (IAM) is a crucial part of securing your network by limiting access to information to only those individuals who need to be able to view said information. For managed services providers (MSPs), IAM is even more important in the context of sensitive client information.

An IAM solution allows administrators to perform the following functions:

a) Alter a user's role
b) Monitor user activities and behavior
c) Generate reports on user activities and behavior
d) Enforce access policies

VII. TOOLS/TECHNOLOGY & IMPLEMENTATION FOR IAM, PAM

When you're implementing an IAM strategy within your MSP, the following three areas should be considered carefully:

A. Policy
B. Identity management
C. Privileged user management

Policy refers to the strategy and guidelines governing how access rights are managed, how access can be requested, and when access should be revoked. Identity management involves the establishment of specific digital identities for each person. Finally, privileged user management refers to the additional controls and processes that should be implemented to protect the most critical and sensitive system operations. To support the goals of the three key elements of an IAM strategy, there are also several features and capabilities you should seek out in the software you choose to employ.

1) Biometric Authentication
2) MULTI-FACTOR Authentication (MFA)
3) Context-Aware Access Control
4) Revoke Access
5) Risk-Based Authentication

TOOLS

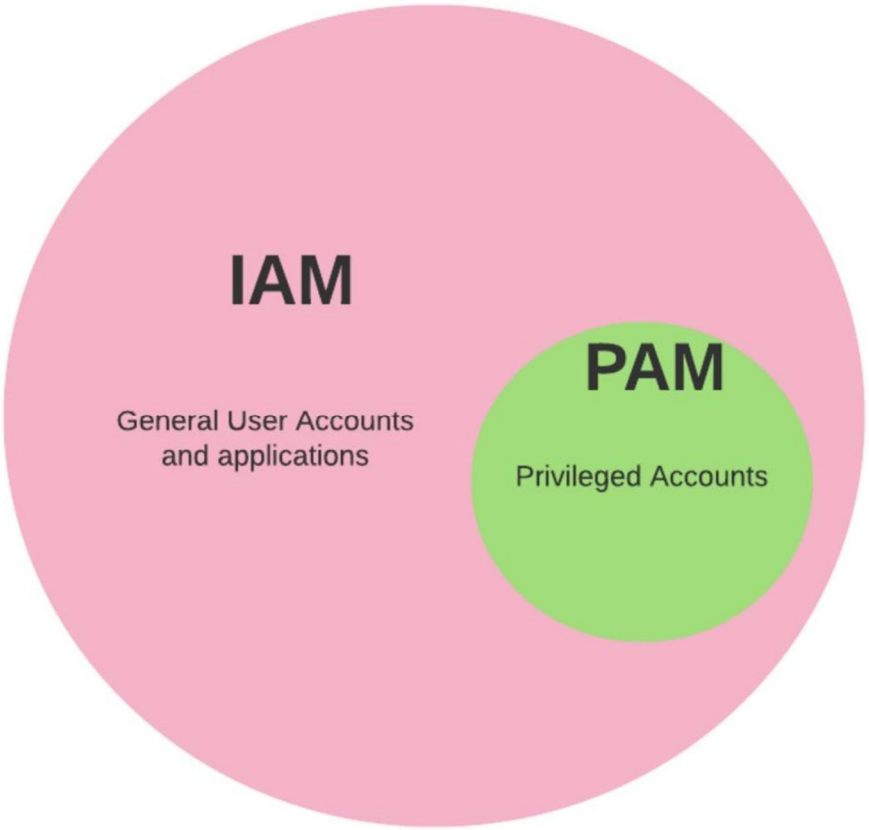
- IDAPTIVE
- CYBERARK
- CENTRIFY
- OKTA
- ONE-LOGIN
- FORGEROCK

Note: On-premise & SaaS both can used as per users case requirements, It's recomended to prefer Cloud solutions.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

VIII. RESULT

The best practice in integration usually is PAM solution to be primarily implemented, followed by a complimentary IAM solution.



IAM & PAM

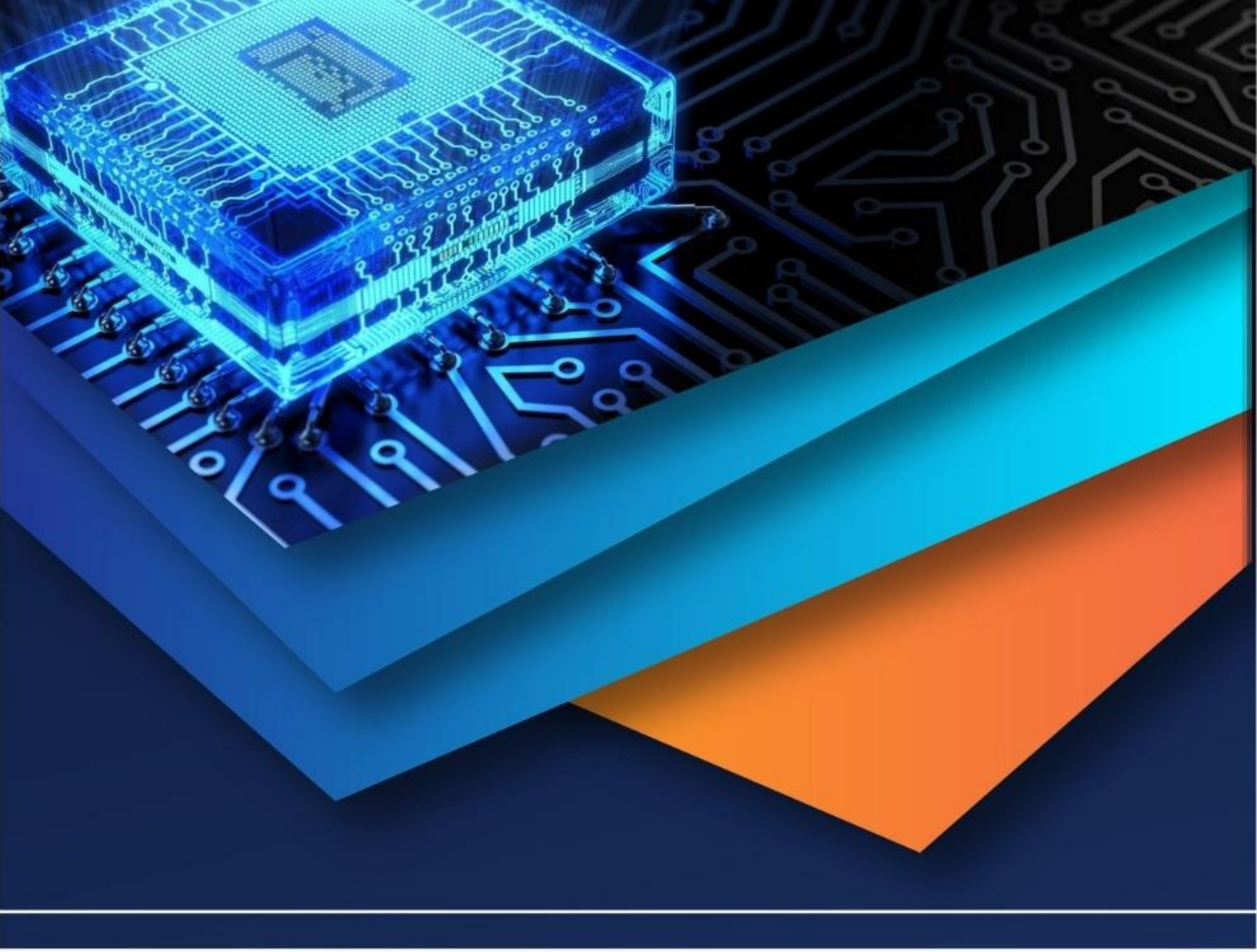
In conclusion, it is clear that if you organization is managing lot of privileged accounts and passwords, along with other CIAM and Workforce IAM capabilities, better to back you system with a good PAM solution integrated to a IAM solution.

IX. FUTURE WORK

On-Premise implemetation of the IAM solution over the site.

REFERENCES

[1] https://backstage.forgerock.com/
[2] https://www.okta.com/developers/
[3] https://www.youtube.com/channel/UC1pQS-4JSrM6GNepeH2nGcA
[4] https://training.cyberark.com/
[5] https://docs.centrify.com/
[6] https://docs.idaptive.com/Content/CoreServices/GetStarted/services-components-overview/UserP ortalOverview.htm



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY