***Report on Identity and Access Management (IAM) and Privileged Access Management (PAM):***

***Author: Vineeth M***

***Date: 18 sep , 2025***

***Summary***

*Identity and Access Management (IAM) is a system that manages all user accounts, ensuring the right people have the right access to systems, apps, and data, by handling account creation, authentication (like passwords or 2FA), authorization (deciding what users can access), and monitoring for security. Privileged Access Management (PAM) is a specialized part of IAM that focuses on high-power accounts, such as admins or root users, keeping them safe with secure password storage, limiting their permissions to only what their role requires, and monitoring or recording everything they do like a CCTV. In short, IAM is the overall gatekeeper for all users, while PAM protects and watches over the “superuser” accounts to prevent misuse or mistakes.*

***Identity Access Management (IAM)***

***Identity and Access Management (IAM)*** *is a security framework that ensures the right people have the right access to the right resources at the right time. It combines two key functions: identity management, which confirms that a user is genuine, and access management, which controls what that user can do once authenticated. IAM systems use tools such as usernames, passwords, multi-factor authentication, and role-based access to verify and manage user permissions. This helps organizations protect sensitive information, prevent unauthorized access, and make user management more efficient. In simple terms, IAM makes sure only trusted people can enter a system and only lets them use what they are allowed to.*

*Identity and Access Management (IAM) ensures that different users have the right level of access to digital resources. One of the main methods used is* ***Role-Based Access Control (RBAC)****, where permissions are given based on a user’s role rather than assigning them individually. For example, in a company, an employee may only access basic work files, a manager may access both team reports and employee data, and an administrator may have full control over the system. By grouping permissions into roles such as "employee," "manager," or "admin," IAM makes access control easier to manage, reduces errors, and increases security. This way, users only get the access they need to do their jobs, and nothing more.*

*It helps organizations verify user identities through authentication, control what users can access via authorization, manage user roles and permissions, and maintain logs for auditing and compliance. Instead of building security features from scratch, developers implement IAM tools like Okta, Microsoft Entra ID, or Ping Identity to efficiently and securely manage user access.*

## ***Core Concepts Related to IAM***

## ***Digital Identities***

*A digital identity is a collection of information about individuals, organisations, or devices that exists online or on a network.*

***Key Attributes / Characteristics***

* *Date of birth*
* *Domain*
* *Email address*
* *IP address*
* *Medical history*
* *Online search activities (browsing history, transactions)*
* *Purchasing history*
* *Social Security Number*
* *Username and password*

***Digital Resources***

*Digital resources are assets that exist in digital form and can be accessed electronically. They are stored, processed, and transmitted using computers and networks.*

***Examples***

* ***APIs*** *— software programs communicate to each other*
* ***Cloud services*** *— online storage or computing platforms*
* ***Databases*** *— organized data storage*
* ***Digital certificates*** *— SSL/TLS certificates for secure communication*
* ***Digital content*** *— images, videos, audio, animations*
* ***Email & communication platforms*** *— Gmail, social media*
* ***Files & documents*** *— Word files, PDFs, spreadsheets*
* ***IoT devices*** *— smart devices that send/receive data online*
* ***Network resources*** *— routers, firewalls, IPs, DNS*
* ***Software applications*** *— cloud, mobile, desktop apps*
* ***Virtual machines & cloud instances*** *— virtual computers on servers*
* ***Web pages & websites*** *— HTML pages, e-commerce sites, blogs*

### ***Identity Management (IdM)***

*Identity management is the process of verifying and confirming who a user, device, or system really is. It ensures that the digital identity presented matches the actual person or entity trying to gain access. This is usually done through credentials such as usernames, passwords, biometrics (fingerprint, face scan), or multi-factor authentication.* **In short, identity management confirms the user is genuine.**

### ***Access Management (AM)***

*Access management comes after identity has been verified. Its job is to decide what that user is allowed to do within the system or application. It uses the confirmed identity to assign permissions, such as whether the user can read data, edit files, or access sensitive resources. For example, an employee may be able to view company documents but not change financial records.* In short, ***access management controls what a verified user can do***

***Latest Tools***

### ***1.Zluri***

*Zluri is a unified access management platform that automates onboarding, offboarding, and app access. It provides* ***zero-touch provisioning****, granting new hires access automatically, and* ***secure offboarding*** *by revoking access when employees leave. It also handles* ***automated access requests*** *from a catalog and manages* ***non-SCIM apps*** *via API integrations.*

### ***2.Okta Workforce Identity***

*Okta centralizes identity management with* ***Single Sign-On (SSO)****,* ***Multi-Factor Authentication (MFA)****, and automated* ***user lifecycle management****. Its* ***adaptive authentication*** *monitors unusual behavior, and reporting tools help with compliance.*

### ***3️.CyberArk Workforce Identity***

*CyberArk combines IAM with* ***Privileged Access Management (PAM)****. It offers* ***password vaulting****,* ***session monitoring****,* ***least privilege access****, and* ***temporary privilege elevation*** *for tasks.*

### ***4️. OneLogin***

*OneLogin simplifies access with* ***SSO****,* ***MFA****, and automated* ***user provisioning/deprovisioning****. Its* ***directory integration*** *ensures consistent profiles, and* ***reporting*** *tracks activity for compliance.*

### ***5.Microsoft Entra ID (Azure AD)***

*Entra ID centralizes cloud and on-premises identity and access management. It provides* ***application protection****,* ***centralized control****,* ***activity monitoring****, and* ***data encryption****, with adaptive security policies.*

***Privileged Access Management (PAM)***

***Privileged Access Management (PAM) is a cybersecurity discipline focused on protecting accounts with elevated powers, such as admin or root accounts, along with privileged processes like automated backups. Unlike normal users, who may only have permission to view data, privileged users can configure, add, change, or delete critical information and system settings. This makes privileged accounts high-value targets for hackers, since compromising them can give attackers full control over sensitive systems. The risks also come from within an organization, where employees might unintentionally expose confidential data by using unauthorized tools. PAM tools and practices secure these accounts by reducing the number of privileged users, protecting admin credentials, enforcing the principle of least privilege, and monitoring privileged activity. In this way, PAM plays a key role in strengthening an organization’s security posture.***

### ***Difference Between PAM and IAM***

*Identity and Access Management (IAM) is the broad practice of securing digital identities and managing access for all users and resources in an organization. Privileged Access Management (PAM), on the other hand, is a specialized subset of IAM that focuses only on accounts with elevated privileges, such as administrators and root users. While both IAM and PAM deal with identity provisioning, authentication, and access control, PAM provides stronger security measures because privileged accounts pose greater risks if compromised. PAM uses advanced techniques such as credential vaults and session recording to tightly control how elevated access is granted and used. Applying these strict measures to all users would make normal daily tasks slow and impractical, which is why IAM and PAM exist as separate but related disciplines.*

## ***Why privileged access management Important***

***Privileged Access Management (PAM) is important because privileged accounts, such as system admin or special service accounts, are very risky. Hackers often target these accounts because their permissions let them access important data, spread malware, or move through the network. Identity-based attacks, where attackers take over user accounts, are increasing. IBM reports that these attacks make up 30% of all security breaches. Breaches using stolen credentials are expensive, costing about USD 4.67 million on average. Insider threats that misuse valid privileges can cost even more, around USD 4.92 million.***

*The number of privileged accounts is growing because of cloud services, AI, IoT devices, and digital transformation. These accounts include human admin accounts and service accounts. Sometimes, teams share these accounts, which makes tracking who does what harder. PAM tools and strategies give organizations* ***visibility and control*** *over these accounts without stopping normal work. Tools like* ***credential vaults****,* ***just-in-time privilege elevation****, and* ***session monitoring*** *help users access what they need safely while keeping hackers and unauthorized users out. By watching privileged activity and enforcing controls, PAM reduces breach risks, protects critical systems, and helps detect suspicious actions. This makes PAM a very important security measure.*

*****How Privileged Access Management (PAM) Works*****

*****Privileged Account Management*****

*Privileged Account Management is the part of PAM that keeps all high-power accounts safe. These are accounts that have more control than normal users, like admin or root accounts. The process starts with* ***discovery****, where all privileged accounts in the system are identified. Next, credentials such as passwords or keys are stored securely in a* ***vault****, and* ***access control*** *ensures that only authorized users can retrieve them. Finally, passwords or keys are* ***rotated regularly*** *to prevent misuse. For example, a server admin who needs to log in requests the password from the PAM vault. The system checks their permission, gives temporary access, and then changes the password automatically afterward.*

***Privilege Management***

***Privilege Management decides what each privileged user can do once they have access. Users don’t get unlimited power; they get only the permissions needed for their role. The process begins with defining roles, like database admin or network admin, and then assigning rights specific to that role. The principle of least privilege ensures users have only the minimum access required to do their job, and permissions are reviewed periodically to make sure they are still necessary. For example, a database admin, can read and write data but cannot delete the server, a network admin, can restart devices but cannot access HR files.***

***Privileged Session Management***

***Privileged Session Management monitors what privileged users actually do while accessing the system. It works like a CCTV for admins, recording and sometimes watching actions in real-time. The system records every session, monitors actions live, and stores logs for audits or compliance reviews. It can even terminate sessions automatically if it detects risky behavior. For example, when an admin logs in to fix a bug, PAM records every command they type. If they try to delete a critical folder by mistake, the system can alert security and pause the session.***

*****Latest Tools*****

### *****1. StrongDM*****

*StrongDM is a cloud-native PAM platform designed for* ***Zero Trust access****, giving IT teams full control over permissions, just-in-time access, and auditing. It simplifies access to databases, servers, Kubernetes clusters, and web apps, logging every user session for compliance reporting. Features include* ***faster onboarding****,* ***secure offboarding****, automated adoption of* ***least privilege policies****, and vendor access management with automatic expiration.*

### *****2️. CyberArk*****

*CyberArk is a comprehensive PAM solution for* ***human and machine identities****, deployed via SaaS or on-premises. It manages privileged credentials, provides* ***just-in-time access****, session recording, adaptive MFA, and SSO. CyberArk supports Zero Trust security but can be complex and costly to implement, and some threat detection features are limited to on-premises deployments.*

### *****3️. Okta ASA (Advanced Server Access)*****

*Okta ASA focuses on* ***cloud-native PAM*** *for servers in multi-cloud environments. It provides* ***team-based role access****, automates onboarding/offboarding, and generates audit logs. However, it only manages* ***servers (SSH/RDP)****, lacks individual credential control, and doesn’t cover apps, databases, or Kubernetes.*

### *****4️. HashiCorp Vault*****

*HashiCorp Vault is a* ***secrets management solution*** *for storing and controlling access to passwords, tokens, and encryption keys. It creates* ***ephemeral credentials*** *that expire automatically, reducing risk from leaked passwords. For full PAM use, it is often paired with HashiCorp Boundary for session management and just-in-time access.*

### *****5️. Delinea (Thycotic & Centrify)*****

*Delinea offers a* ***flexible PAM platform*** *covering credential storage, endpoint security, cloud access, and code security. Its Secret Server securely stores credentials, integrates with Active Directory/LDAP, supports least-privilege access, and provides reporting and automation features like password rotation. It works well in Windows environments but has limited support for cloud-native databases and Kubernetes.*

***Conclusion:*** *IAM (Identity and Access Management) manages user identities and controls access to applications, ensuring the right people can access the right resources safely. PAM (Privileged Access Management) protects high-privilege accounts by enforcing least-privilege access, just-in-time permissions, and session monitoring. Together, IAM and PAM strengthen organizational security by managing both regular and critical access efficiently.*