IAM Models, Concepts, Technologies, and Tools for a FinTech Organization

The main purpose of this white paper is to highlight the importance of Identity and Access Management in Fintech organizations and to outline its implementation strategies.

INTRODUCTION

Identity and access management (IAM) is a vital framework of business processes, policies, and technologies that enable the management of digital identities and access rights across systems, applications, and data. On a fundamental level, IAM systems are designed to allow, deny, limit, and revoke access to individuals and resources through identification, authentication, and authorization. With an IAM framework, IT managers can control user access to information in organizations. (Gittlen & Rosencrance, 2021)

FinTech organizations, on the other hand, are organizations that make use of technologies to modify, enhance, and automate financial services for customers; they can also be referred to as businesses that utilize AI, big data, and encrypted blockchain technology to facilitate highly secure transactions in the internal network.

FinTech business owners have felt increased regulatory and organizational need to protect access to corporate resources. “Over 64% of financial services companies have 1,000+ sensitive files open to every employee. This puts them at risk of non-compliance with regulations like the EU General Data Protection Regulation (GDPR), Sarbanes-Oxley (SOX), and California Consumer Privacy Act (CCPA) — which all require strict controls on sensitive information. Violators could face prison and (in the case of GDPR) up to €20 million or 4% of global revenues in fines.” - *Varonis*. Therefore, they can no longer depend on manual and error-prone processes to assign and track user privileges. IAM automates these tasks and enables granular access control and auditing of all corporate assets on-premises. (Gittlen & Rosencrance, 2021)

IAM MODELS

Access control models define the rules and principles governing how access rights are granted, revoked, and managed within an organization. These models provide a framework for implementing security policies and ensuring that access to resources is restricted based on predefined criteria.

Common Access Control Models Include:

- **Role-based Access Control (RBAC):** This access control model uses a user's role to determine what access to grant them. Roles can be tailored to each user to maintain a least privilege policy so access can be revoked once no longer needed. (Priyadarshini, 2021)
- **Attribute-Based Access Control (ABAC):** Here, access is granted based on attributes associated with users, resources, and environmental conditions (for example, location). Attributes can include job roles, department, location, time of day, etc.
- **Discretionary Access Control (DAC):** This type of access control uses a subject's identity or group they belong to manage access; we refer to this as discretionary because a subject with certain permissions can pass that permission. (Priyadarshini, 2021)
- **Mandatory Access Control (MAC):** MAC is a type of access control in which access rights are regulated by a central authority based on multiple levels of security. It works on a hierarchy pattern, which means in a team everyone needs to be separated into different groups based on their roles and responsibilities and information they're cleared to view.

IAM CONCEPTS

Access control models provide a structured approach to managing access rights, reducing the risk of unauthorized access, and ensuring compliance with regulatory requirements. They enable organizations to implement least-privilege access principles and maintain a secure environment.
Authentication: This is a process of verifying the identity of a user (person or device) attempting to access a FinTech system after they have provided their login credentials. It requires using credentials such as username and password, fingerprints, and certificates.

How it Works: Authentication in data systems involves the user providing credentials such as username, password, biometrics, or security token. The system then verifies the user's credentials and grants access to authorized resources. If verification fails, access is denied.

Importance: Strong authentication methods prevent unauthorized access to sensitive financial data and accounts, protecting customer funds and preventing fraudulent transactions. FinTech regulations, like PCI DSS, mandate specific authentication practices to ensure data security. Multi-factor authentication (MFA) and risk-based approaches hinder fraudulent activities, making unauthorized access more difficult. Streamlined authentication processes with user-friendly interfaces enhance the user experience by allowing quick and secure access.

Implementation Strategies: FinTech companies should require complex passwords, regular changes, and multi-factor authentication for sensitive actions and high-risk logins. IAM systems can use risk assessment tools to adjust authentication requirements based on the risk level of login attempts.

Multi-Factor Authentication (MFA): MFA is a method of authentication that requires two or more verification factors. It's a core concept of a strong identity and access management (IAM) policy and includes something users are (biometrics), something they know (password, passphrase), and something they have (token, certificate).

How it works: MFA requires additional verification information (factors) from the user. One common factor is One-Time Passwords (OTPs), which are 4–8-digit codes sent via email, SMS, or a mobile app. A new code is generated periodically based on a seed value assigned to the user during registration.

Importance:

The main benefit of MFA is that it enhances organization security by requiring users to identify themselves with more than a username and password. This helps protect against brute-force attacks and theft of login credentials, providing increased confidence in the organization's safety from cyber threats.

Authorization: Authorization is the act of allowing or refusing access rights and permissions to verified entities, like users, applications, or systems, depending on their confirmed identity and specified privileges. Unlike authentication, which confirms the identity of a user or entity, authorization decides which actions or resources the authenticated identity can utilize. (Bhattacherji, 2023) After an entity has been identified and authenticated, authorization takes place to determine the specific actions they are permitted to perform. Access controls are utilized to implement authorization. This ensures users only have access to the specific data, functionalities, and resources relevant to their roles and responsibilities.

How it works: When a user tries to access a resource or perform an action in the FinTech platform, the system checks their permissions based on their role. If the user has the necessary permissions, access is granted. If not, access is denied, and the user may see an error message or be redirected to request permissions.

Importance: Effective authorization is vital for FinTech organizations because it enhances security, reduces fraud risk, ensures regulatory compliance, and improves operational efficiency. It restricts access to authorized users, prevents unauthorized data activities, limits fraudulent transactions, meets regulatory requirements, and streamlines user workflows.

Implementation Strategies: Implementing robust authorization practices in FinTech IAM requires careful planning. User roles should be clearly defined, and specific permissions should be assigned to each role. An appropriate authorization model should be chosen based on the organization's needs, and the principle of least privilege should be followed. Periodic reviews of user roles and permissions are essential to minimize the risk of unauthorized access.

IAM Technologies and Tools for a FinTech Organization:

OAuth is an open-standard authorization protocol that provides applications the ability to secure designated access. OAuth doesn’t share password data; however, it uses authorization tokens to verify an identity between consumers and service providers. OAuth also allows granular permission levels. (Sobers, 2022)

How it works:

There are 3 main characters in an OAuth transaction: the user, the consumer, and the service provider.

The user shows intent to access a service, then the consumer gets permission from the service provider for the request token and a secret. The secret is then used to prevent request forgery. The consumer uses the secret to sign each request so that the service provider can verify that the permission is coming from the consumer application. The user is redirected to the service provider. The user permits the service provider then the consumer obtains an access token which finally allows consumer access to resources. (Sobers, 2022)

OKTA: This is an identity and access management company that provides cloud software that helps companies manage and secure user authentication into applications and for developers to build identity controls into applications, websites, and web services. Okta runs in the cloud, on a secure, reliable, extensively audited platform, which integrates deeply with on-premises applications, directories, and identity management systems. (Okta, 2023)

How it works: Okta’s features include Single Sign-On (SSO), LDAP integration, Provisioning, Active Directory (AD), the centralized off-boarding of users, multifactor authentication (MFA), mobile identity management, and flexible policies for organization security and control. All these functions are brought together through a network of pre-integrated applications called the Okta Integration Network (OIN). The OIN provides diverse integration options, enabling SSO login for every app your users need to access during their workday.

CONCLUSION

In the finance industry, Identity and Access Management (IAM) platforms are crucial for balancing security and efficient access to financial systems. IAM systems play a vital role in safeguarding financial transactions and upholding trust. As FinTech organizations undergo digital transformation, IAM's importance in maintaining the security and integrity of financial processes remains significant.

References

Bhattacherji, A. (2023, June 21). *Identity and Access Management Basic Concepts*. Retrieved from Medium: https://medium.com/identity-and-access-management-iam/identity-and-access-management-basic-concepts-2c0e1f2767be

Gittlen, S., & Rosencrance, L. (2021, August). *What is identity and access management? Guide to IAM*. Retrieved from TechTarger: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

Okta. (2023, May 9). *What is Okta and What Does Okta Do?* Retrieved from Okta Help Center: https://support.okta.com/help/s/article/what-is-okta?language=en_US

OneLogin. (n.d.). *What is Multi-Factor Authentication (MFA) and How Does it Work?* Retrieved from OneLogin: https://www.onelogin.com/learn/what-is-mfa

Priyadarshini, P. (2021, April 14). *7 Types Of Identity Management Access Controls*. Retrieved from Idenhaus: https://idenhaus.com/7-types-of-identity-management-access-controls/

Sobers, R. (2022, June 29). *What is OAuth? Definition and How it Works*. Retrieved from Varonis: https://www.varonis.com/blog/what-is-oauth

CONTRIBUTORS

Kenechukwu Obiagazie	CG/24/0219
Folarin Favour Awolola	CG/24/0211
Pearl Olaoluwa Aina	CG/24/0212
Sanusi Abimbola	CG/24/0213
Amosun Ifawuyi	CG/24/0214
Abigail Masela	CG/24/0215
Mariam Ali	CG/24/0216
Violet Mutesi	CG/24/0217
Janice Kemunto	CG/24/0218
Onyinye Okonkwo	CG/24/0220