International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

AUTOMATING USER PROVISIONING WITH IDENTITY PROVIDERS

Sandhya Rani Koppanathi
itsmeksr01@gmail.com

Abstract

Integrating Identity Providers (IdPs) like Okta and Azure Active Directory (Azure AD) with Salesforce, so that user provisioning happens automatically in the background is becoming a big trend as more organizations look to simplify their identity management & access control through automation. Of course, this approach not only makes the org more secure, but also increases efficiency by saving a lot of time and effort that would have been spent on these mundane tasks to create user accounts. This is enabled through Single Sign-On (SSO) and Just-in-Time (JIT) provisioning, that makes it possible to provide immediate access in a secure manner based on identity so users can get straight into the resources they need. This paper investigates the methods, advantages and challenges of automating Salesforce with an external Integrating Identity Provider (IdP) to guide organizations intending on implementing or evolving their Identity and Access Management (IAM) strategies. The paper also features real-world examples and best practices to demonstrate how these technologies can be practically deployed for the betterment of organizations.

Keywords: User Provisioning, Salesforce, Identity Providers, Okta, Azure AD, Single Sign-On, Just-in-Time Provisioning, Single Sign-On (SSO), Just-in-Time (JIT), Identity and Access Management (IAM), Automation, Security.

I. INTRODUCTION

Protecting access to cloud applications (like Salesforce) is a significant part of an enterprise security strategy in the digital economy. User provisioning (creating, maintaining and deleting user accounts) has traditionally been a manual task left to the hands of IT administrators. Yet, as enterprises grow and adoption of cloud-based applications rise, provisioning manually becomes unsustainable resulting in inefficiencies and exposures to security risks or compliance challenges.
The good news is that there is a great solution to these problems, of integrating Identity Providers (IdPs) like Okta and Azure Active Directory (Azure AD) with Salesforce. Through automatically provisioning the users as well activating Single Sign-On (SSO) and Just-in-Time (JIT) provision organizations can make sure that resource management is simpler, secure while providing access to necessary resources for their employees in real-time. This paper explores the technical aspects of automating user provisioning in Salesforce through IdPs, the benefits of such integration, and best practices for implementation.

II. IDENTITY PROVIDERS AND THEIR ROLE IN USER PROVISIONING

Identity Providers (IdPs) are essential components of modern IAM systems, offering centralized authentication and authorization services. IdPs like Okta and Azure AD provide a secure and scalable framework for managing user identities across multiple applications, including Salesforce.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

2.1 Overview of Okta and Azure AD

- Okta: Okta is a leading cloud-based Identity Provider that provides a range of IAM services, including SSO, Multi-Factor Authentication (MFA), and automated user provisioning. Okta integrates with numerous applications, including Salesforce, to enable seamless user access and management.
- Azure AD: Azure AD is Microsoft's cloud-based identity and access management service, integrated with the Azure platform. It offers SSO, MFA, and user provisioning capabilities, making it a popular choice for organizations using Microsoft services alongside Salesforce.

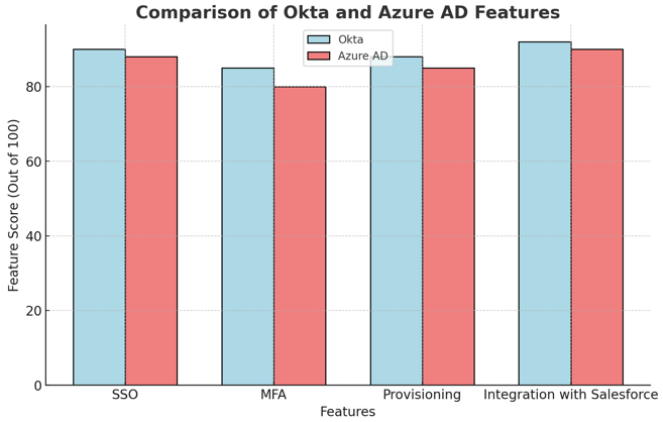

Fig.1. Comparison of Okta and Azure AD features

2.2 Key Functions of Identity Providers in User Provisioning

IdPs perform several critical functions in the user provisioning process:

- Authentication: IdPs authenticate users by verifying their credentials before granting access to applications like Salesforce.
- Authorization: Based on predefined policies and user roles, IdPs authorize user actions within Salesforce, ensuring that users only have access to the resources they need.
- Provisioning: IdPs automate the creation, updating, and deactivation of user accounts in Salesforce, often through JIT provisioning or scheduled synchronization.
- SSO: SSO allows users to access Salesforce and other integrated applications with a single set of credentials, reducing the need for multiple logins and improving the user experience.

III. AUTOMATING USER PROVISIONING IN SALESFORCE

Automating user provisioning in Salesforce using IdPs like Okta and Azure AD involves several steps, including setting up SSO, configuring JIT provisioning, and ensuring secure communication between Salesforce and the IdP.

3.1 Single Sign-On (SSO) Integration

SSO is a foundational component of automating user provisioning. By integrating SSO, organizations can streamline the user authentication process, allowing users to access Salesforce with their existing corporate credentials.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

3.1.1 SSO Implementation in Salesforce with Okta and Azure AD

The implementation of SSO in Salesforce through Okta or Azure AD involves several key steps:

- Step 1: Configure SSO Settings in Salesforce: Begin by configuring the SSO settings in Salesforce. This includes setting up the SSO provider (Okta or Azure AD), defining the identity provider URL, and uploading the IdP's certificate for secure communication.
- Step 2: Configure the IdP (Okta or Azure AD): In Okta or Azure AD, create an application that represents Salesforce. Configure the application's SSO settings, including the Salesforce URL, relay state, and attribute mappings. Ensure that the IdP is configured to pass the necessary user attributes (e.g., username, email, roles) to Salesforce.
- Step 3: Test the SSO Integration: After configuration, test the SSO integration by logging in to Salesforce through the IdP. Verify that the login process works smoothly and that users are correctly authenticated and authorized based on their roles.

3.1.2 Benefits of SSO Integration

- Enhanced Security: SSO reduces the risk of password-related security breaches by allowing users to log in once with their corporate credentials, which are typically protected by strong authentication methods like MFA.
- Improved User Experience: Users benefit from a seamless login experience, reducing the need to remember multiple passwords and minimizing login-related friction.
- Centralized Access Management: SSO centralizes access management, making it easier for administrators to enforce security policies and monitor access across all applications, including Salesforce.

3.2 Just-in-Time (JIT) Provisioning

JIT provisioning is a powerful feature that automates the creation of user accounts in Salesforce the moment a user attempts to log in via SSO. This approach ensures that user accounts are only created when needed, reducing the administrative burden of pre-provisioning accounts.

3.2.1 How JIT Provisioning Works

When JIT provisioning is enabled, the following process occurs:

- Step 1: User Initiates Login: A user initiates a login to Salesforce via the IdP (e.g., Okta or Azure AD) using SSO.
- Step 2: IdP Sends SAML Assertion: The IdP authenticates the user and sends a SAML assertion to Salesforce. This assertion contains user attributes such as username, email, and roles.
- Step 3: Salesforce Creates or Updates User Account: Salesforce receives the SAML assertion and either creates a new user account or updates an existing one based on the attributes provided. The user is then granted access to Salesforce with the appropriate permissions.

3.2.2 Configuring JIT Provisioning in Salesforce

To configure JIT provisioning in Salesforce:

- Step 1: Enable JIT Provisioning in Salesforce: Navigate to the Single Sign-On settings in Salesforce and enable JIT provisioning. Specify the user profile and role to be assigned to users who are provisioned via JIT.
- Step 2: Configure Attribute Mappings: Ensure that the IdP is configured to send the necessary attributes in the SAML assertion, such as username, email, and any custom attributes required by Salesforce.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

- Step 3: Test the Provisioning Process: Test the JIT provisioning process by attempting to log in to Salesforce as a new user. Verify that the user account is created or updated correctly, and that the user is assigned the appropriate profile and role.

3.2.3 Advantages of JIT Provisioning

- Efficiency: JIT provisioning eliminates the need for administrators to manually create user accounts in Salesforce, reducing administrative overhead and speeding up the onboarding process.
- Scalability: JIT provisioning scales easily with the organization, automatically creating user accounts as needed, regardless of the number of users.
- Cost-Effective: By only provisioning accounts when users need them, JIT provisioning helps organizations avoid unnecessary account creation, potentially reducing licensing costs.

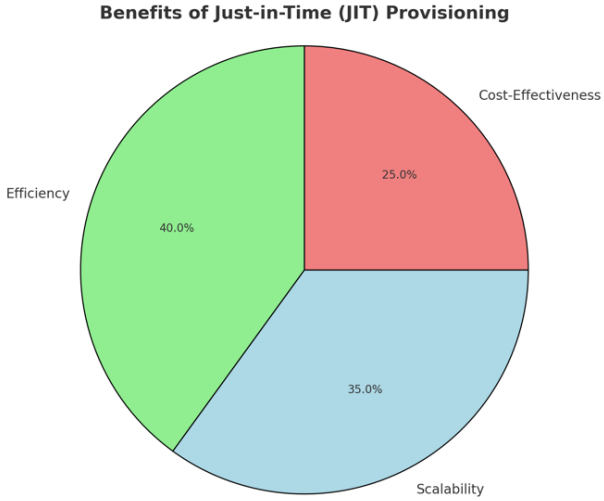

Fig.2. Benefits of using JIT Provisioning

IV. SECURITY CONSIDERATIONS IN AUTOMATING USER PROVISIONING

While automating user provisioning through IdPs offers numerous benefits, it also introduces security considerations that organizations must address to protect their Salesforce environments.

4.1 Securing SSO and JIT Provisioning

The security of SSO and JIT provisioning depends on several factors, including the strength of the authentication mechanisms used by the IdP and the integrity of the attribute mappings.

4.1.1 Multi-Factor Authentication (MFA)

Implementing MFA is essential to secure SSO and JIT provisioning. MFA requires users to provide two or more forms of verification before accessing Salesforce, significantly reducing the risk of unauthorized access even if credentials are compromised.

- Okta MFA: Okta supports a wide range of MFA options, including SMS, email, authenticator apps, and biometric factors. Organizations can enforce MFA policies based on user roles, location, and device trust levels.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

- Azure AD MFA: Azure AD offers MFA through methods like phone call, text message, and mobile app notifications. Azure AD's Conditional Access policies allow for granular control over when MFA is required, enhancing security without compromising user experience.

4.1.2 Securing Attribute Mappings

Attribute mappings define how user attributes from the IdP are translated into Salesforce user profiles and roles. It is crucial to ensure that these mappings are secure and accurate to prevent privilege escalation or unauthorized access.

- Least Privilege Principle: Apply the principle of least privilege by ensuring that users are assigned the minimum necessary permissions based on their roles. Avoid mapping attributes that could grant excessive access.
- Regular Audits: Regularly audit attribute mappings to verify that they align with organizational policies and do not expose the system to security risks.

4.2 Compliance and Data Privacy

Automating user provisioning through IdPs must also comply with data privacy regulations, such as GDPR, HIPAA, and CCPA, which govern the handling of personal data.

4.2.1 Data Minimization

Ensure that only the necessary user attributes are shared between the IdP and Salesforce. Avoid sending unnecessary personal data in SAML assertions or other provisioning messages to reduce the risk of data breaches and ensure compliance with data minimization principles.

4.2.2 Secure Data Transmission

All data exchanged between the IdP and Salesforce should be encrypted using strong encryption protocols, such as TLS 1.2 or higher. This ensures that sensitive information, such as user credentials and personal data, is protected from interception and unauthorized access during transmission.

4.3 Monitoring and Logging

Monitoring and logging are critical for detecting and responding to security incidents related to user provisioning. Organizations should implement comprehensive logging and monitoring strategies to track provisioning activities and identify potential threats.

4.3.1 Log Management

Both Salesforce and the IdP should generate detailed logs of all provisioning activities, including account creation, updates, and deletions. These logs should be securely stored and retained according to organizational policies and compliance requirements.

4.3.2 Real-Time Monitoring

Real-time monitoring of provisioning activities allows organizations to detect and respond to suspicious behavior, such as unauthorized account creation or privilege escalation. Integration with Security Information and Event Management (SIEM) systems can enhance real-time monitoring capabilities.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

V. BEST PRACTICES FOR IMPLEMENTING AUTOMATED USER PROVISIONING

Implementing automated user provisioning in Salesforce through IdPs requires careful planning and adherence to best practices to ensure success. The following best practices can help organizations achieve secure and efficient provisioning processes.

5.1 Develop a Clear Provisioning Policy

Before implementing automated provisioning, organizations should develop a clear policy that defines how user accounts should be managed. This policy should outline the roles and permissions that users should be granted, the criteria for provisioning and deprovisioning accounts, and the security measures to be applied.

- Role-Based Access Control (RBAC): Implement RBAC to simplify the management of user permissions. By assigning users to predefined roles based on their job functions, organizations can ensure that users have appropriate access without the risk of overprovisioning.
- Policy Review: Regularly review and update the provisioning policy to ensure it remains aligned with organizational goals and compliance requirements.

5.2 Perform Regular Audits

Regular audits of user accounts and provisioning activities are essential to maintain security and compliance. Audits help identify inactive or orphaned accounts, verify that users have appropriate access, and detect any deviations from the provisioning policy.

- Automated Audits: Leverage automation tools to perform regular audits, reducing the administrative burden and ensuring consistent checks across the organization.
- Compliance Audits: Conduct compliance audits to verify that provisioning practices meet regulatory requirements, such as GDPR, HIPAA, or CCPA.

5.3 Enable Deprovisioning

Automated deprovisioning is as important as provisioning. When a user leaves the organization or changes roles, their access to Salesforce and other applications should be promptly revoked to prevent unauthorized access.

- Deprovisioning Triggers: Configure the IdP to automatically trigger deprovisioning based on events such as employee termination or role change. Ensure that all access rights are removed in a timely manner.
- Grace Periods: Implement grace periods for deprovisioned accounts to allow for account reactivation, if necessary, while ensuring that access to sensitive data is restricted.

5.4 Test and Validate Provisioning Processes

Before rolling out automated provisioning to the entire organization, thoroughly test and validate the provisioning processes. This includes testing SSO integration, JIT provisioning, and deprovisioning workflows to ensure they function as expected.

- Pilot Testing: Start with a pilot group of users to test the provisioning processes and identify any issues or areas for improvement. Use feedback from the pilot group to refine the implementation.
- Validation Checks: Implement validation checks to verify that user accounts are correctly provisioned and that access rights are appropriately assigned.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

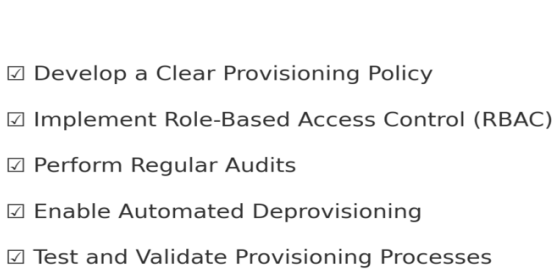

Fig.3. Best Practices for implementing Automated User Provisioning

VI. CASE STUDIES: SUCCESSFUL IMPLEMENTATION OF AUTOMATED USER PROVISIONING

The following case studies illustrate how organizations have successfully implemented automated user provisioning in Salesforce through IdPs, achieving significant improvements in security and efficiency.

6.1 Case Study: Large Financial Institution

6.1.1 Background

A large financial institution with thousands of employees worldwide needed to streamline its user provisioning process for Salesforce. The institution faced challenges in managing user access across multiple regions and ensuring compliance with financial regulations.

6.1.2 Solution

The institution implemented automated user provisioning using Okta as the Identity Provider. SSO was configured to allow employees to access Salesforce with their corporate credentials. JIT provisioning was enabled to automate the creation of user accounts as employees logged in for the first time.

To enhance security, the institution implemented MFA for all Salesforce users and configured Okta to enforce role-based access control (RBAC) policies. Regular audits were conducted to ensure compliance with regulatory requirements.

6.1.3 Outcomes

Improved Efficiency: The automated provisioning process significantly reduced the time and effort required managing user accounts, allowing the institution to focus on core business activities.

Enhanced Security: The combination of SSO, JIT provisioning, and MFA provided a robust security framework, reducing the risk of unauthorized access to sensitive financial data.

Regulatory Compliance: The institution achieved compliance with financial regulations by implementing automated audits and ensuring that all provisioning activities were logged and monitored.

6.2 Case Study: Global Manufacturing Company

6.2.1 Background

A global manufacturing company with operations in multiple countries needed to automate user provisioning for Salesforce to support its growing workforce. The company faced challenges in managing user access across various regions and ensuring that users were granted appropriate permissions based on their roles.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

6.2.2 Solution

The company implemented Azure AD as its Identity Provider and integrated it with Salesforce for SSO and JIT provisioning. Azure AD's Conditional Access policies were used to enforce MFA for all Salesforce users, enhancing security across the organization.

To ensure that user accounts were consistently provisioned based on job roles, the company implemented RBAC within Azure AD and configured attribute mappings to automatically assign users to the correct profiles in Salesforce.

6.2.3 Outcomes

- Scalable Provisioning: The automated provisioning process enabled the company to scale its workforce efficiently, ensuring that new employees were granted timely access to Salesforce resources.
- Increased Security: The use of MFA and RBAC provided a strong security framework, reducing the risk of unauthorized access and ensuring that users only had access to the resources they needed.
- Operational Efficiency: The automated provisioning process reduced the administrative burden on IT staff, allowing them to focus on strategic initiatives rather than manual account management.

VII. FUTURE TRENDS IN AUTOMATED USER PROVISIONING

As organizations continue to adopt cloud-based applications and services, several trends are likely to shape the future of automated user provisioning.

7.1 AI-Driven Provisioning

Artificial intelligence (AI) is expected to play an increasingly important role in user provisioning, enabling more intelligent and adaptive provisioning processes. AI can analyze user behavior and access patterns to dynamically adjust provisioning policies, ensuring that users have access to the resources they need while minimizing security risks.

7.2 Zero Trust Architecture

The shift towards Zero Trust architecture will impact user provisioning practices, requiring continuous verification of user identities and access rights. This approach will ensure that access is granted based on real-time assessments of risk and trust, rather than relying on one-time authentication.

7.3 Integration with Identity-as-a-Service (IDaaS)

As organizations increasingly adopt Identity-as-a-Service (IDaaS) solutions, automated user provisioning will become more integrated with cloud-based IAM services. IDaaS solutions offer scalability and flexibility, allowing organizations to manage user identities and access rights across multiple cloud-based services and applications.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

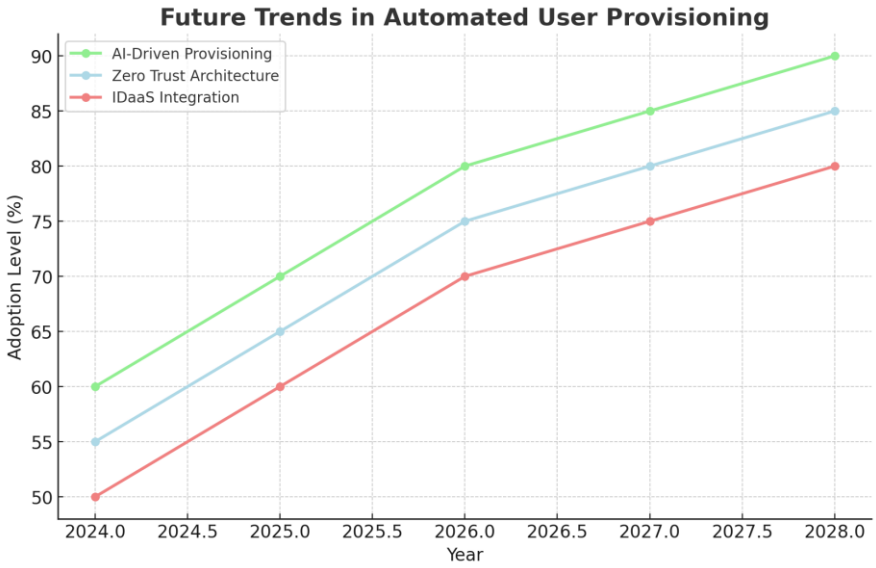

Fig.4. Future Trends in Automated User Provisioning

VIII. LIMITATIONS/CHALLENGES

The challenges discussed below highlights the need for careful planning, robust security practices, and continuous evaluation to effectively implement and manage IAM systems in an organization:

8.1 Integration Complexity

Integrating IAM systems with existing IT infrastructure can be complex, especially when dealing with legacy systems. The compatibility between different systems and the IAM solution often requires custom solutions, increasing the time and cost of implementation.

8.2 Scalability Issues

As organizations grow, scaling IAM solutions can become challenging. The need to manage increasing numbers of users, applications, and data types without degradation in performance or service disruptions is a major concern.

8.3 Security Risks

While IAM systems enhance security, they also present new risks. Any vulnerabilities in the IAM system can expose all connected systems to security breaches. Moreover, managing access rights, particularly in large organizations, can lead to errors that might inadvertently grant excessive permissions to users.

8.4 Compliance and Regulatory Challenges

Adhering to regulatory requirements is a critical challenge for IAM solutions. Regulations often require specific security measures and data handling procedures that must be integrated into the IAM strategy, requiring continuous updates and audits.

8.5 User Experience and Adoption

Balancing security with user convenience is a common challenge. Stringent security measures can sometimes hinder user experience, leading to resistance from users. Ensuring the system is user-friendly while maintaining high security standards is crucial for successful adoption.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

8.6 Cost Implications
The initial setup, ongoing maintenance, and periodic upgrades of IAM systems involve significant financial investment. For some organizations, especially small to medium-sized enterprises, these costs can be prohibitive.

8.7 Technical Expertise
Deploying and managing IAM solutions requires specialized knowledge. Organizations often need to invest in training for IT staff or hire new personnel with the requisite expertise, which adds to the overall cost.

8.8 Privacy Concerns
Managing and protecting user data within an IAM system is paramount. There is a constant challenge to ensure that personal data is handled securely in compliance with privacy laws, which can vary widely by region.

8.9 Vendor Dependence
Relying on external vendors for IAM solutions can lead to dependency risks, including lack of control over certain aspects of the IAM service, potential service discontinuity, and exposure to vendor-specific threats.

8.10 Technology Evolution
Keeping pace with rapid technological advancements and cybersecurity threats is another challenge. IAM systems must continually evolve to address new security challenges and leverage emerging technologies, requiring ongoing investment and strategy updates.

IX. CONCLUSION

Automating user provisioning in Salesforce through the integration of Identity Providers like Okta and Azure AD is a critical component of modern IAM strategies. By leveraging technologies such as SSO and JIT provisioning, organizations can streamline user management, enhance security, and ensure compliance with regulatory requirements.
This paper has explored the key methodologies, benefits, and challenges associated with automating user provisioning in Salesforce through IdPs. By following best practices and learning from real-world case studies, organizations can implement secure and efficient provisioning processes that meet their unique needs.
As the digital landscape continues to evolve, organizations must remain vigilant in their approach to user provisioning. Emerging trends such as AI-driven provisioning, Zero Trust architecture, and IDaaS integration will shape the future of IAM, enabling organizations to adapt to new challenges and opportunities.

9.1 Effective Integration Strategies
The paper concludes that effective integration of IAM systems with existing IT infrastructures is crucial but complex. It highlights the need for careful planning and customization to ensure seamless integration, particularly with legacy systems that might not support modern IAM features.

International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

9.2 Scalability and Flexibility
The conclusion emphasizes that IAM solutions must be scalable and flexible to adapt to organizational growth. This involves supporting an increasing number of users and applications without compromising performance, which requires robust architecture and foresight in system design.

9.3 Security Enhancements and Risks
While IAM systems significantly enhance security by managing user identities and access, they also introduce new security risks. The paper suggests continuous assessment of the IAM system's security measures and regular updates to defend against emerging threats.

9.4 Regulatory Compliance
Maintaining compliance with various data protection and privacy regulations is critical. The conclusion points out the challenges in keeping up with regional and industry-specific regulations and recommends implementing compliance as a core feature of the IAM strategy.

9.5 User Experience and System Adoption
Balancing security measures with user convenience is essential for the successful adoption of IAM systems. The conclusion notes that user experience should not be compromised and recommends strategies for user engagement and training to promote system adoption.

9.6 Cost Management
Implementing and maintaining IAM systems can be costly. The paper advises that organizations should carefully evaluate the costs against the potential benefits, considering both direct financial impacts and indirect benefits such as increased productivity and reduced security risks.

9.7 Necessity of Technical Expertise
Managing IAM solutions requires specialized knowledge. The conclusion emphasizes the importance of having trained IT personnel dedicated to the deployment and management of IAM systems or outsourcing certain elements to reputable vendors.

9.8 Privacy Management
Ensuring the privacy of user data within IAM systems is paramount. The paper concludes that organizations must enforce strict data protection policies and employ advanced encryption methods to secure personal and sensitive data.

9.9 Vendor Relationship Management
Dependency on external vendors for IAM solutions can be a double-edged sword. The conclusion suggests establishing strong vendor management practices to mitigate risks associated with service levels, data sovereignty, and vendor lock-in.

9.10 Keeping Pace with Technology
The conclusion stresses the importance of continuously updating IAM systems to keep pace with technological advances and evolving security landscapes. This includes adopting new technologies that enhance the functionality and security of IAM systems.

REFERENCES

1. Sharif, A., Carbone, R., Ranise, S., & Sciarretta, G. (2019). "A wizard-based approach for secure code generation of single sign-on and access delegation solutions for mobile native apps." In press.
2. Subbarao, D., Raju, B., Anjum, F., Rao, C., & Reddy, B. (2021). "Microsoft azure active directory for next level authentication to provide a seamless single sign-on experience." Applied nanoscience. In press.
3. Mainka, C., Mladenov, V., & Schwenk, J. (2014). "Do not trust me: Using malicious IdPs for analyzing and attacking single sign-on." 2016 IEEE European symposium on security and privacy (EuroS&P), 321-336. In press.
4. Kirschnick, J., Calero, J., Wilcock, L., & Edwards, N. (2010). "Toward an architecture for the automated provisioning of cloud services." IEEE Commun. Mag., 48, 124-131. Unpublished.
5. Wettinger, J., Andrikopoulos, V., Leymann, F., & Strauch, S. (2018). "Middleware-oriented deployment automation for cloud applications." IEEE transactions on cloud computing, 6, 1054-1066. Unpublished.
6. Saatkamp, K., Breitenbücher, U., Kopp, O., & Leymann, F. (2019). "Method, formalization, and algorithms to split topology models for distributed cloud application deployments." Computing, 102, 343-363. Unpublished.
7. Ramamoorthi, L., & Sarkar, D. (2019). "Single sign-on implementation: Leveraging browser storage for handling tabbed browsing sign-outs." Unpublished.
8. Buyya, R., & Barreto, D. (2015). "Multi-cloud resource provisioning with Aneka: A unified and integrated utilisation of microsoft azure and amazon EC2 instances." 2015 International conference on computing and network communications (CoCoNet), 216-229. Unpublished.
9. Li, Y., Han, Z., Zhang, Q., Li, Z., & Tan, H. (2020). "Automating cloud deployment for deep learning inference of real-time online services." IEEE INFOCOM 2020 - IEEE conference on computer communications, 1668-1677. In press.
10. Karthikeyan, S. (2018). "Automated provisioning and performance fine-tuning." Unpublished.
11. Weinmeister, P. (2019). "Automating your business with workflow." Practical salesforce development without code. Unpublished.
12. Liu, X., Liu, J., Wang, W., & Zhu, S. (2018). "Android single sign-on security: Issues, taxonomy and directions." Future gener. Comput. syst., 89, 402-420. In press.
13. Nguyen, D., Wermke, D., Acar, Y., Backes, M., Weir, C., & Fahl, S. (2017). "A stitch in time: Supporting android developers in writing secure code." Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. In press.