Review of Identity and Access Management Systems and Potential Contributions of Self-Sovereign Identity

Aditya Poddar 2101CS05
Dhruv Kumar Agrawal 2101CS26

April 21, 2025

1 Abstract

This paper provides an in-depth analysis of existing Identity and Access Management (IAM) systems, their weaknesses in the form of complexity, security risks, and absence of user control. It introduces upcoming technologies such as AI, blockchain, and privacy-enhancing models, with Self-Sovereign Identity (SSI) as a potential decentralized, user-centric model providing more security, privacy, and manageability. The analysis is further extended to future issues in the form of quantum-resistant cryptography, especially applicable to sectors such as healthcare and banking. The paper also promotes the implementation of standards such as SCIM with Single Sign-On (SSO) to offer more security, compliance, and operating efficiency in controlling access to critical infrastructure. Overall, the research indicates a transition towards more secure, privacy-enhancing, and user-centric IAM models, while considering the technical and adoption challenges that still prevail.

2 Introduction

Identity and Access Management (IAM) is a security cornerstone for enterprises, yet it continues to pose numerous challenges — especially as cyber threats rise and the demand for secure remote access grows. This paper investigates the limitations of existing IAM methods and explores Self-Sovereign Identity (SSI) as a potential new framework. Drawing on current literature and enterprise requirements across security, compliance, operability, technology, and user experience, the study highlights the advantages of SSI — a decentralized, password-less identity system that gives users control over their digital credentials through cryptographic attestations stored in digital wallets.

3 Literature review

Identity and Access Management (IAM) has long been viewed as a key pillar of enterprise cybersecurity. It ensures that only authorized users can access specific resources, helping organizations maintain both security and compliance. However, traditional IAM systems are increasingly criticized for being overly complex, inefficient, and vulnerable—especially in the era of remote work and widespread adoption of cloud infrastructure.

The Fig. 1 provided information about the IAM configuration phase, as well as the IAM operation phase. “Identity Access Management” (IAM) can support handling permissions, which manage how AWS resources can access users. IAM is also known as “role-based access controls” (RBAC), through which cloud customers can easily assign individual function, which is related to a set of permission to access other functions, data stores, as well as open Internet. Roles of strict IAM can be constructed for those functions which are limited to communicating with those important requirements to handle their activities

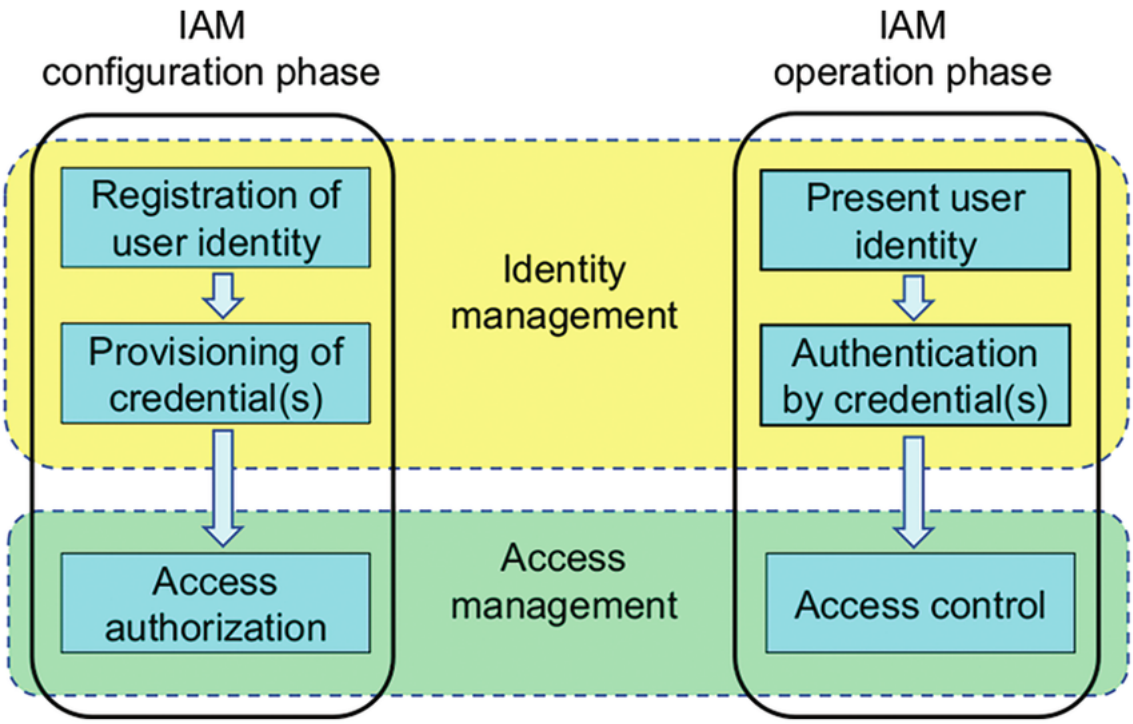
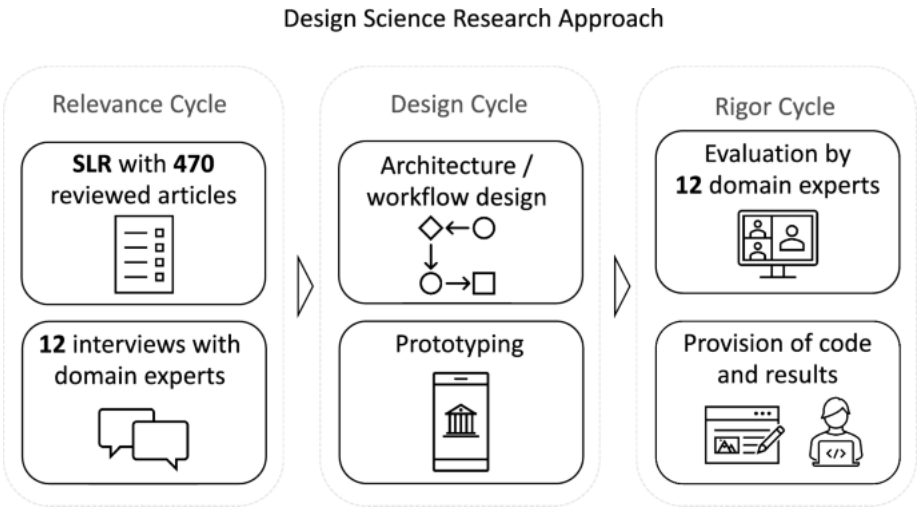


Figure 1: . IAM phases

3.1 Importance in Maintaining Security Systems within Organizations

Singh, Thakkar, and Warraich (2023) underscore the critical importance of IAM in protecting digital assets across modern organizations. Their study reveals how poorly implemented IAM poli-

cies—particularly those relying on static credentials and outdated access control—can lead to major security breaches. They call for stronger IAM frameworks that better address evolving security demands and the growing need for remote authentication in a post-pandemic world.



The six studies discussed in this research paper investigate the potential of using future technologies—Artificial Intelligence (AI), blockchain, Distributed Ledger Technology (DLT), improved authentication processes, and workflow integration—to improve Identity and Access Management (IAM) systems. Although all the studies recognize the potential of these technologies, they also recognize serious challenges, which are mainly in terms of security, privacy issues, and technical complexity.

Key Points from the Paper:

- **AI in IAM**: AI facilitates the automation of tasks like password management and adding new users. AI can enhance security as well by monitoring the user behavior and identifying suspicious patterns that can indicate the presence of threats. Privacy and safety issues still exist, particularly regarding how AI impacts confidentiality of data.
- **Advanced Authentication Mechanisms**: Many papers propose that sophisticated authentication schemes, i.e., multi-factor authentication or biometrics, can greatly enhance IAM security. Implementing these solutions, however, requires a tremendous amount of investment and technical effort, particularly in the ever-changing cloud computing scenario.
- **Blockchain and Distributed Ledger Technology (DLT)**: Blockchain enables individuals to hold identity information in a secure and personal manner without relying on central authority. DLT offers an immutable and common ledger for managing entry and encouraging accountability and transparency. The technologies are, however, new and are plagued by scalability.

- **Workflow Integration**: Implementing automated workflows in IAM systems can automate user access provisioning and revocation, hence increasing efficiency and decreasing human errors. This is especially in serverless computing environments, where IAM systems tend to be strained.

3.2 Privacy-enhanced User-Centric Identity Management

From a user-centered angle, Ahn, Ko, and Shehab (2009) were early pioneers in enhancing privacy within identity systems. Their research introduced models that gave users more control over their digital credentials, directly addressing concerns around centralized IAM—namely, the lack of autonomy and personal data privacy. Though their work predates more recent developments, it laid important groundwork for today's decentralized identity approaches.

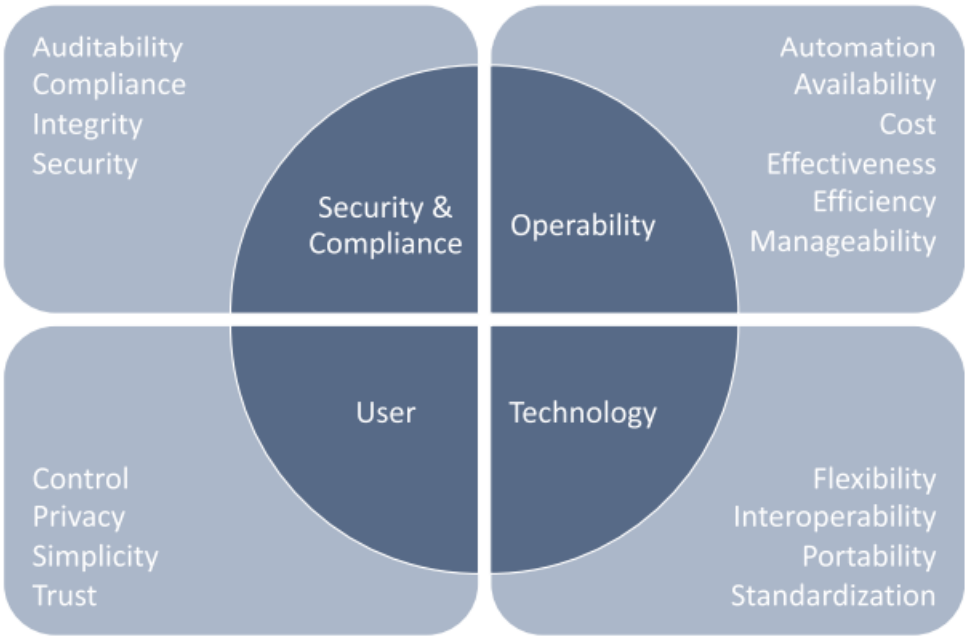


Figure 2: Requirements for an enterprise IAM system: consolidated results after the SLR and the evaluation with experts

- The paper discusses a method of managing privacy preferences in terms of categories. The method is designed to improve privacy management in user-centered digital identity systems, particularly the Identity Metasystem. It touches on the challenge of assigning privacy to individual claims or entire information cards, which can be cumbersome and time-consuming. To address this, the authors propose clustering claims. This enables easier and more consistent privacy labeling, making the process easier, avoiding redundant effort, and enabling users to have better control over their personal data.

- The authors demonstrate their solution with a prototype identity selector implemented in Java.

The prototype is equipped with privacy labels on identity claims and makes use of privacy policies, such as P3P Lite, to manage and compare privacy selections in an orderly manner. The system allows users to specify their privacy preferences on a per-category basis and provides clear warnings in case of user preference-party policy conflicts. The primary goal is to facilitate privacy protection without rendering it inconvenient to use in usual, user-managed identity management systems.

- The paper highlights the importance of users controlling their digital identities and information and solving privacy issues that occur in identity transactions. By using privacy labels to show the sensitivity of claims and bundling claims, the method helps manage privacy better and solve conflicts between what users want and the policies of whom they rely on. The paper also discusses future work, which includes testing the usability of the system and improving privacy management features to provide better and easier privacy protection in identity systems.

3.3 A Review of Identity and Access Management Business Requirements and Potential Benefits of Self-Sovereign Identity.

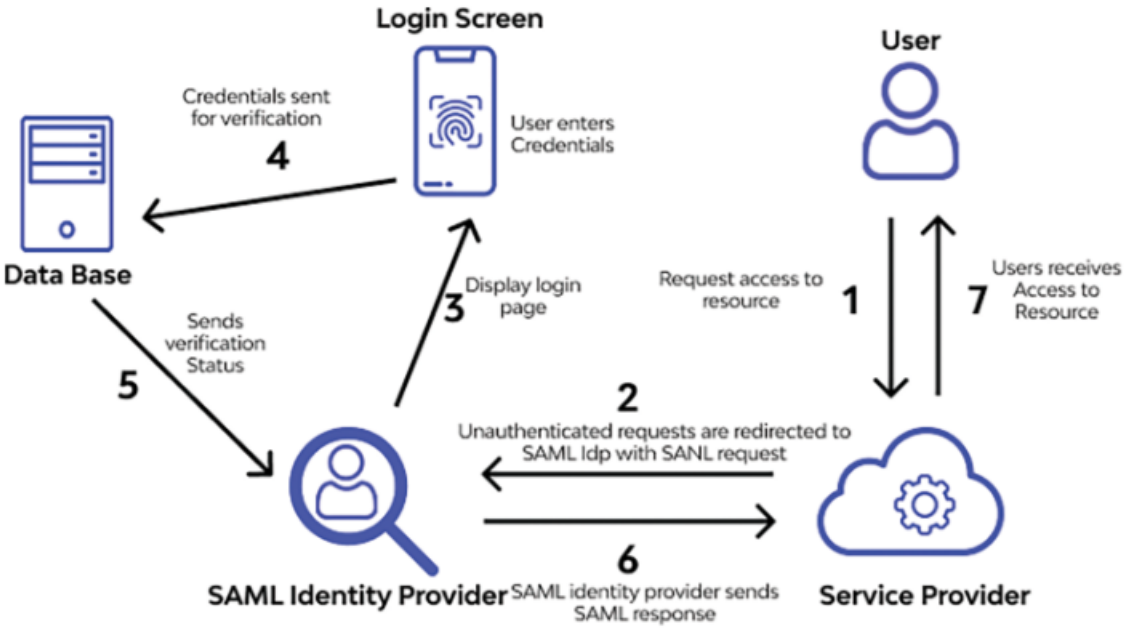


Figure 3: SAML authentication process

Glöckler et al. (2023) conducted a detailed analysis of IAM requirements in enterprise settings, using a systematic literature review and expert interviews. They classified IAM needs into four areas: security and compliance, operability, technology, and user experience. Their findings highlighted

critical gaps in current systems—particularly with scalability and user manageability—and introduced Self-Sovereign Identity (SSI) as a compelling alternative. SSI removes the need for centralized authorities by enabling users to store verifiable credentials in personal digital wallets, offering a passwordless and decentralized approach. While the authors demonstrated the potential of an SSI-based IAM prototype, they also concluded that SSI, though promising, is not a cure-all for the complexity of modern enterprise IAM.

- The study considers thoroughly investigating and enhancing the requirements for user enterprise Identity and Access Management (IAM) systems. It emphasizes the significance of security, compliance, manageability, efficiency, standardization, and user trust.
- Expert interviews and systematic literature review (SLR) are used to find prominent sets of requirements. These sets are then combined based on the recommendations of the experts to form a more practical set of categories.
- The final set of IAM requirements are divided into four general categories:
  - **Security and Compliance:** Includes safeguarding information, compliance with regulations, and minimizing risk.
  - **Operability:** Emphasizes manageability, flexibility, availability, and simplicity of system administration.
  - **Technology:** Includes interoperability, standardization, scalability, and technical robustness.
  - **User:** Prioritizing usability, privacy, control by the user, and system trust.
- A prototype based on Self-Sovereign Identity (SSI) concepts is developed to demonstrate how decentralized digital identities can be handled in business environments.
- The SSI-based prototype allows employees to establish secure links with their digital wallets through QR codes. The codes assist in cryptographic key generation and enable secure communication.
- Credential issuance in the proof-of-concept is done by the HR department publishing credential schemas and definitions to a blockchain, and issuing verifiable credentials (VCs) to employees, who keep them in their wallets.
- Workers can establish themselves by offering cryptographic proof (verifiable presentations) showing only required characteristics, utilizing zero-knowledge proofs (ZKPs) for added security and privacy.

- The system is revocation-enabled, allowing for timely revocation of credentials when employee attributes change, thus maintaining trust and compliance.
- Industry experts indicate that SSI integration into commercial IAM solutions can significantly improve security, privacy, and management in business IAM systems. Benefits in this regard include minimized password dependency and better control over the user.
- The identified challenges are low legacy IAM vendor adoption, user comprehension of SSI principles, and technical maturity concerns.
- The literature review and the expert opinions show that SSI is an appropriate solution for resolving most IAM challenges, especially those of security, privacy, interoperability, and user experience.
- The study highlights that SSI is not a universal fit but a viable solution that has the potential to augment current IAM frameworks, especially in cases of the need for decentralized control and increased privacy.
- Literature review encompasses a wide range of issues ranging from cybersecurity, blockchain identity, biometric authentication, privacy issues, and new trends such as zero-knowledge proofs and attribute-based access control.
- The ability of blockchain technology to facilitate decentralized identity management is brought to the fore, though SSI is not necessarily blockchain-dependent, with the flexibility of deployment.
- The research calls for an end-to-end approach to digital identity management, integrating SSI concepts with current systems to enhance security, usability, and compliance.
- Future research areas involve examining wider stakeholder views, the convergence of SSI with IoT and smart devices, comparing SSI with conventional solutions, and investigating its place in emerging paradigms such as zero trust architectures.
- The overall conclusion emphasizes that SSI provides a privacy-enhancing, adaptable, and user-centric solution to enterprise IAM, where technical hurdles need to be addressed and larger-scale adoption encouraged by continuous development.
- The lengthy list of references suggests that the discipline includes a vast array of fields. It includes technical models, everyday problems, laws and regulations, and innovative ideas for managing digital identity.

In summary, the evolution of IAM is moving from centralized, administrator-controlled models toward more decentralized, user-empowered solutions. While traditional IAM remains widely used, 2 there is growing academic and industry interest in SSI as organizations search for scalable, secure, and privacy-respecting identity frameworks.

3.4 Potential Impact of Quantum-Resistant Cryptography on Future IAM Security in Healthcare and Banking

As quantum computing is expanding at a faster rate, the cryptographic foundations of the current Identity and Access Management (IAM) systems are facing a severe test. Post-quantum cryptography or quantum-resistant cryptography aims to develop quantum-resistant algorithms to safeguard sensitive data from quantum attacks. This report discusses the future impact of quantum-resistant cryptography on IAM security for the banking and healthcare sectors.

The Quest for Quantum-Resistant Cryptography

ECC and RSA, the traditional cryptography primitives, can be attacked with Shor's algorithm, which can be efficiently run by a quantum computer. This makes confidentiality of authentication tokens, patient records, financial data, and other sensitive information that IAM systems process vulnerable. All this needs to be migrated to quantum-resistant primitives to protect from future attacks through quantum computing.

Healthcare IAM Security Implications

Enhanced Data Protection Healthcare infrastructures keep very sensitive patient data encrypted with cryptography protocols. The application of quantum-resistant cryptography will ensure patient records, diagnosis data, and medical data remain secure even after the post-quantum era.

Enhancing Compliance Regulatory conditions such as HIPAA and GDPR demand strong data security measures. Quantum-resistant algorithms will help healthcare organizations remain compliant by providing strong defense mechanisms that will not fall prey to emerging computational attacks.

Challenges and Opportunities

- **Integration Complexity:** It is highly complex to integrate quantum-resistant algorithms with existing IAM infrastructure, including massive protocol upgrades like OAuth and SAML, and legacy systems.

- **Performance Considerations:** Certain post-quantum algorithms take longer to process and have larger key sizes, which can affect system performance.
- **Future-Proofing:** Quantum-resistant cryptography can be adopted early to future-proof healthcare data security and reduce the need for costly overhauls in the future.

Implications for IAM Security in Banks

Securing Financial Transactions Banks heavily rely on cryptographic protocols for secure transactions, authentication, and anti-fraud protection. Quantum-resistant cryptography will grant such operations immunity to future quantum-based attacks, and therefore transaction integrity and customer confidence.

Protecting Customer Data Customer identities, transaction history, and account information are all valuable assets. The shift from quantum-vulnerable algorithms will reduce dangers of data theft and identity theft.

Industry and Regulatory Standards Banks have to comply with strict security standards (e.g., FFIEC guidelines, PCI DSS). Deployment of quantum-resistant cryptography aligns with changing regulatory expectations and industry best practices.

Challenges and Opportunities

- **Implementation Timeline:** The transition to quantum-resistant algorithms should be carefully planned to minimize disruptions.
- **Interoperability:** Compatibility between various banking systems and third-party integrations must be offered.
- **Innovation Catalyst:** Quantum-resistant cryptography can potentially serve as an innovation catalyst for biometric authentication, behavioral analysis, and AI-based security features.

Strategic Considerations

- **Hybrid Approaches:** Blending classical and quantum-resistant algorithms during periods of transition can offer multi-layered security.
- **Research and Development:** Ongoing research on efficient, scalable post-quantum algorithms is a priority.

- **Standards Development:** Collaboration with standards organizations (e.g., NIST) will facilitate wide-scale adoption and interoperability.

Quantum-resistant cryptography will be one of the pillars of IAM security best practices of the future in healthcare and banking. It will increase data confidentiality, integrity, and compliance, protecting valuable assets from quantum attacks in the future. Integration, performance, and standardization challenges exist, but early adoption and ongoing research will allow organizations to build robust, future-proof identity management systems.

3.5 Integrating Identity and Access Management for Critical Infrastructure: Ensuring Compliance and Security in Utility Systems

This report analyzes the security stance of utility organizations handling NERC critical infrastructure information, with an emphasis on the shortcomings of current umbrella-level Single Sign-On (SSO) solutions like Azure Active Directory (Azure AD). It suggests the implementation of System for Cross-Domain Identity Management (SCIM) as a strategic addition to impose fine-grained, role-based access controls based on NERC CIP standards on hybrid cloud environments like Azure, AWS, and on-premises data centers.

Background

Utility providers of critical infrastructure are experiencing increasing levels of cybersecurity threats that demand robust access control solutions. While SSO solutions like Azure AD provide centralized authentication, these are inadequate in terms of granularity necessary for imposing strict role-based access controls (RBAC) necessary to enable NERC CIP compliance. These deficiencies can lead to unauthorized access, leakage of data, and non-compliance.

To address these demands, organizations are exploring advanced identity management technologies with granular control, automation, and compliance capability across complex hybrid cloud infrastructures.

subsubsection*Limitations of Current SSO Solutions

- **Limited Granularity:** SSO is primarily intended for user authentication but does not strictly implement fine-grained role-based authorization, especially for critical NERC data.
- **Manual Role Management:** Role modifications or employee turnover typically must be updated manually, which raises the risk of misconfigurations.

- **Inconsistent Enforcement:** Inconsistencies in the enforcement of access policies between different cloud and on-premises environments can potentially create security loopholes.
- **Audit Challenges:** Lack of complete, centralized provisioning and access change logs makes auditing for compliance difficult.

Suggested Solution: Integration of SCIM

Overview

SCIM is an open, standardized protocol that is designed to automate role management, deprovisioning, and user provisioning between multiple systems. Integration with current identity management systems can significantly enhance security and compliance by enabling:

  - **Automated Role-Based Access Control:** Dynamic user assignment and revocation according to organizational policies.
  - **Centralized Management:** Single, unified control of user identity and permissions across hybrid cloud deployments.
  - **Real-Time Updates:** Real-time reflection of employees' changes in access rights, reducing window for unauthorized access.
  - **Enhanced Auditability:** Detailed records of provisioning operations facilitate compliance and incident investigations.

  Implementation Strategy

  The joining is a two-step process:

    1. **Broad Accessibility via SSO:** Users log in through SSO for seamless login experiences on platforms.
    2. **Fine-grained Control with SCIM:** Once the identity is confirmed, SCIM enforces role-based permissions to restrict access to sensitive NERC data and critical infrastructure controls to authorized personnel.

  This multi-layered approach balances ease of use and security so that ease of use does not compromise control over valuable assets.

Advantages of SCIM Integration

* **Improved Security:** Accurate, automated access controls minimize the threat of insider attacks and outside intrusions.)item **Regulatory Compliance:** Comprehensive

audit trails and auto-provisioning improve NERC CIP standard compliance like CIP-005 (Electronic Security Perimeter) and CIP-007 (System Security Management).

* **Operational Efficiency:** Automation eliminates manual administrative efforts, decreasing errors and releasing resources.
* **Agility:** Rapid response to personnel changes ensures continuous security and compliance.

Challenges and Considerations

* **System Compatibility:** Legacy systems can be supported by SCIM with upgrades or middleware.
* **Configuration Complexity:** SCIM processes require proper configuration and ongoing maintenance to prevent misconfigurations.
* **Monitoring and Auditing:** Security information and event management (SIEM) tools must be integrated with for end-to-end monitoring.
* **Training:** Staff should be trained on new equipment and procedures to perform at their best.

Recommendations

* Offer detailed examination of existing systems for SCIM compatibility.
* Use a phased deployment strategy focusing on business-critical data and systems. Implement strict role definition and access control measures in accordance with NERC guidelines.
* Integrate SCIM logs into SIEM solutions to enable centralized monitoring. Review and revise access policies and system settings on an occasional basis.
* Offer regular training and awareness sessions to administrators and users.

Using SCIM in hybrid cloud infrastructures provides a strategic benefit in having granular, automated, and compliant access controls applied to NERC-critical information. It overcomes the shortcomings of traditional SSO products, improves cybersecurity posture, and provides continuous compliance with regulatory requirements. Utility organizations that adopt this solution will be better equipped to protect their critical infrastructure from emerging cyber threats while maintaining operational efficiency and regulatory compliance.

References

Ahn, G-J, Moonam Ko and Mohamed Shehab. 2009. Privacy-enhanced user-centric identity management. In *2009 IEEE International Conference on Communications*. IEEE pp. 1–5.

Chatterjee, Suchismita. N.d. "Integrating Identity and Access Management for Critical Infrastructure: Ensuring Compliance and Security in Utility Systems." . Forthcoming.

Glöckler, Jana, Johannes Sedlmeir, Muriel Frank and Gilbert Fridgen. 2024. "A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity." *Business & Information Systems Engineering* 66(4):421–440.

Krishnapatnam, Mahendra. 2025. "Cutting-Edge AI Techniques for Securing Healthcare IAM: A Novel Approach to SAML and OAuth Security." *International Journal of Computing and Engineering* 7(2):39–50.

Singh, Chetanpal, Rahul Thakkar and Jatinder Warraich. 2023. "IAM identity Access Management—importance in maintaining security systems within organizations." *European Journal of Engineering and Technology Research* 8(4):30–38.

(Ahn, Ko and Shehab, 2009) (Glöckler et al., 2024) (Singh, Thakkar and Warraich, 2023) (Krishnapatnam, 2025) (Chatterjee, N.d.)'