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

Suchismita Chatterjee

suchi5978@gmail.com
Tx, USA

Abstract

In the utility industry, particularly within the gas and electric sectors, where both physical and software assets are distributed nationwide, securing vast amounts of NERC data stored across on-premises and cloud infrastructures is a critical challenge. To ensure the security of this data, it is essential to adhere to the NERC (North American Electric Reliability Corporation) standards, specifically the BCSI (Bulk Electric System Cyber System Information) standard. The BCSI standard mandates that organizations identify gaps, prioritize risks, and mitigate vulnerabilities based on their identified severity (Ten et al., 2007). The complexity of managing such an environment, combined with stringent operational standards, led to the development of NERC's regulatory frameworks. These frameworks aim to assess system vulnerabilities and provide remediation guidelines grounded in best practices for cybersecurity. However, a notable gap exists between the control frameworks defined by regulatory standards and the practical implementation required from a development standpoint. As a result, companies often face significant data breaches, jeopardizing national security. A key requirement in the BCSI standard is the identification and tagging of "crown jewel" NERC assets, followed by the creation of secure, isolated gateways to restrict access. Only authorized personnel or entities should be allowed access to these critical assets and the data they store, which introduces significant challenges related to data segregation and access control management.

For large organizations, implementing these standards—such as access control, IAM(Identity and Access Management), and SSO (Single Sign-On)—becomes even more complex. However, maintaining strict adherence to the BCSI standards and ensuring robust security measures are in place to manage access effectively is crucial to safeguarding sensitive NERC data and mitigating cybersecurity risks.

Keywords: NERC Certification, Identity and Access Management (IAM), Single Sign-On (SSO), System for Cross Domain Identity Management (SCIM), Utility Sector Cybersecurity, Access Control, Role-Based Access Control (RBAC), Critical Infrastructure Protection (CIP), Data Security, Regulatory Compliance, Cloud Security, IT and OT Integration, NERC Critical Infrastructure Protection Standards, Just-In-Time (JIT) Access, Privileged Access Management (PAM), Data Segmentation, Role-Based Security, Risk Mitigation in Utilities, Access Governance, Enterprise Security Frameworks.

I.INTRODUCTION

The utility industry, encompassing essential sectors such as gas and electric power, serves as the backbone of modern society, delivering critical services that ensure daily life functions seamlessly. As these industries increasingly embrace digital transformation, the challenge of managing and securing sensitive data becomes more complex. Particularly, data associated with the North American Electric Reliability Corporation (NERC) is vital due to its role in safeguarding the reliability and security of the bulk electric system. With the ongoing digitization of physical assets and the migration of critical data to hybrid infrastructures spanning on-premises systems and public clouds such as AWS and Microsoft Azure, ensuring robust security is paramount to protect against cyber threats and maintain uninterrupted services.

The utility sector faces unique hurdles in managing NERC-related data across distributed and diverse infrastructures. Critical systems such as Supervisory Control and Data Acquisition (SCADA), operational technology (OT), and IT infrastructures require unified security frameworks to prevent unauthorized access or exploitation. NERC addresses these challenges through its Critical
Infrastructure Protection (CIP) standards, including the Bulk Electric System Cyber System Information (BCSI) requirements. These standards emphasize protecting critical cyber assets—the "crown jewels" of utility systems—by enforcing stringent access controls that align with the principle of least privilege, restricting access solely to authorized personnel.

However, translating these regulatory directives into actionable security measures is particularly challenging in hybrid environments that span legacy systems and modern cloud platforms. Public clouds such as AWS and Azure provide comprehensive Identity and Access Management (IAM) tools, yet their layered and modular architectures often require careful alignment with NERC's compliance standards. For instance, managing access for a large organization with tens of thousands of employees necessitates granular control to ensure only NERC-certified personnel can access specific repositories, while other data repositories remain accessible to non-certified personnel. Flat architectures and traditional Role-Based Access Control (RBAC) models often fall short in such scenarios, leading to potential gaps in data security.

This paper explores the adoption of IAM and Single SignOn (SSO) solutions in hybrid cloud environments, with a focus on AWS and Azure, to address the complexities of securing NERC data. AWS and Azure both provide advanced IAM frameworks with features like group-based access control, SSO integration with Active Directory, and automation tools such as System for Cross-Domain Identity Management (SCIM). These capabilities enable organizations to implement a two-phase access model: first, granting umbrella-level authentication through SSO for system-wide login access, and second, enabling granular role-based access with SCIM to enforce stricter controls for NERC-certified personnel.

Furthermore, the scalability and automation features of AWS and Azure allow for real-time synchronization of user roles and permissions, reducing the risk of unauthorized access and enhancing compliance with BCSI standards. For example, Azure Active Directory integrates JIT provisioning to ensure real-time updates of user roles, while AWS IAM provides policies for fine-grained access control tailored to BCSI requirements. Both platforms enable monitoring and auditing of access controls, ensuring consistent policy enforcement across geographically dispersed teams and infrastructures.

This paper demonstrates how leveraging the IAM and SSO capabilities of AWS and Azure, combined with regulatory-aligned frameworks like SCIM, can help utility organizations bridge the gap between NERC compliance requirements and practical implementation. By employing these technologies, organizations can achieve robust, scalable, and compliant access control for NERC data, mitigating cybersecurity risks while maintaining operational efficiency and protecting critical infrastructure.

I.STRENGTHENING NERCDATA SECURITY WITH SSO AND SCIMINTEGRATION

In today's utility sector, effective access management is crucial to safeguarding sensitive NERC data while maintaining operational efficiency. Single Sign-On (SSO) has emerged as a powerful tool for centralizing access control, simplifying authentication, and providing real-time synchronization of user credentials. Features like Just-InTime (JIT) provisioning ensure that changes in user roles, new employee additions, and naming conventions are instantly updated across the system. By integrating SSO with Active Directory, organizations can authenticate employees centrally, granting them minimal security group access for basic system visibility. However, while SSO ensures valid credentials at a high level, it does not inherently provide the granular access control necessary to isolate critical NERC environments and restrict access to only certified personnel.

To overcome these limitations, integrating SSO with the System for Cross-Domain Identity Management (SCIM) offers a comprehensive solution for achieving both centralized access management and detailed role-based security. This integration enables organizations to meet the principle of least privilege by precisely defining user roles and aligning them with specific access permissions, ensuring that only NERC-certified personnel can access sensitive data while others are restricted to non-critical repositories.

1. Addressing the Limitations of Traditional Access Models

Traditional access control systems, such as Active Directory, often rely on an "All-in" or "All-out" approach when assigning access to users within a group. This lack of granularity poses a significant challenge for organizations handling NERC data, as it could inadvertently allow unauthorized users to access critical repositories. For example, in a company with tens of thousands of employees, granting broad group-level access risks exposing NERC data to noncertified personnel, thereby compromising security and regulatory compliance.

SCIM addresses this limitation by enabling the creation of specialized user groups and allowing customized role assignments based on real-time needs. These user groups are dynamically managed, with roles that can be updated, created, or revoked automatically through SCIM's synchronization mechanisms. By connecting these user groups to backend databases, SCIM ensures that only certified individuals with appropriate roles can access, edit, or manage NERC data.

2. A Two-Phase Access Management Model

The integration of SSO and SCIM is most effective when implemented using a two-phase access management approach, which balances broad system access with strict data security controls:

•Phase 1 – Universal System Access via SSO

- In the initial phase, SSO provides an umbrella login mechanism, allowing all employees to access the system with basic credentials. This "Shift Left" methodology simplifies authentication and provides all users with limited access to general system dashboards or non-sensitive repositories.

- SSO authenticates users through a centralized mechanism, ensuring that all entries into the system are verified at a high level. This reduces administrative overhead and streamlines the onboarding process for new employees.

•Phase 2 – Granular Role-Based Access via SCIM

- The second phase introduces granular role management through SCIM, where user groups are aligned with specific job responsibilities. For NERC-certified personnel, SCIM enforces strict access controls, allowing them to interact with NERC-related repositories while restricting others to noncritical data.

- SCIM automates the management of these user groups, ensuring real-time updates to roles and permissions. This automation reduces manual intervention, enhancing efficiency and minimizing the risk of misconfiguration.

3.The Benefits of SCIM Integration

SCIM integration provides several advantages that make it an essential component of a secure and scalable access management framework for NERC data:

- Granular Access Control: SCIM allows for detailed role assignments, ensuring that users can only access data relevant to their roles. This aligns with the principle of least privilege and significantly reduces the attack surface.

- Real-Time Synchronization: Automated synchronization processes, such as cron jobs, ensure that user roles and permissions remain current and accurate, reflecting changes in real time.

- Seamless Integration with Active Directory: SCIM works in tandem with Active Directory to create a unified access management solution, bridging the gap between centralized authentication and detailed role enforcement.

- Automated Workflows: SCIM facilitates access approval workflows, where leaders or managers validate and approve access requests. This ensures that only a limited number of trusted individuals can access NERC data, making the system more secure and easier to monitor.

4. Access Verification and Governance

SCIM also enhances governance by embedding access validation within the approval process. Access requests are directed to team leaders or managers who are familiar with the specific requirements of NERC certification. These managers review and approve requests, ensuring that only individuals with verified credentials and relevant job responsibilities can gain access to critical data. This controlled process minimizes the risk of unauthorized access and ensures accountability within the system.

5. Bridging the Gap Between SSO and NERC Compliance

The combination of SSO and SCIM creates a robust framework for managing access in large utility organizations. SSO simplifies access management at a high level, while SCIM ensures that granular controls are in place to protect NERC data. By implementing this two-phase approach, organizations can achieve:

- Enhanced Compliance: Alignment with NERC BCSI standards through strict access control mechanisms.

- Scalability: Efficient management of access across large, distributed teams and hybrid environments.

- Operational Efficiency: Reduced administrative overhead through automation and streamlined workflows.

By leveraging the capabilities of both SSO and SCIM, utility organizations can ensure the security of their NERC environments while maintaining operational efficiency and regulatory compliance. This integrated approach addresses the unique challenges of managing access in hybrid cloud infrastructures like AWS and Azure, ultimately safeguarding critical infrastructure against cyber threats.

II.INTEGRATING AZURE AD,SSO, AND SCIM FOR SECURE AND GRANULAR ACCESS MANAGEMENT

The diagram (Fig 1) complements the paper by visually illustrating the integration of identity and access management (IAM) technologies—Azure Active Directory (Azure AD), Single Sign-On (SSO), and System

for Cross-Domain Identity Management (SCIM)—to address the challenges of securing NERC and non-NERC data in hybrid environments. Here's how it fits into the key themes and discussions in the paper:

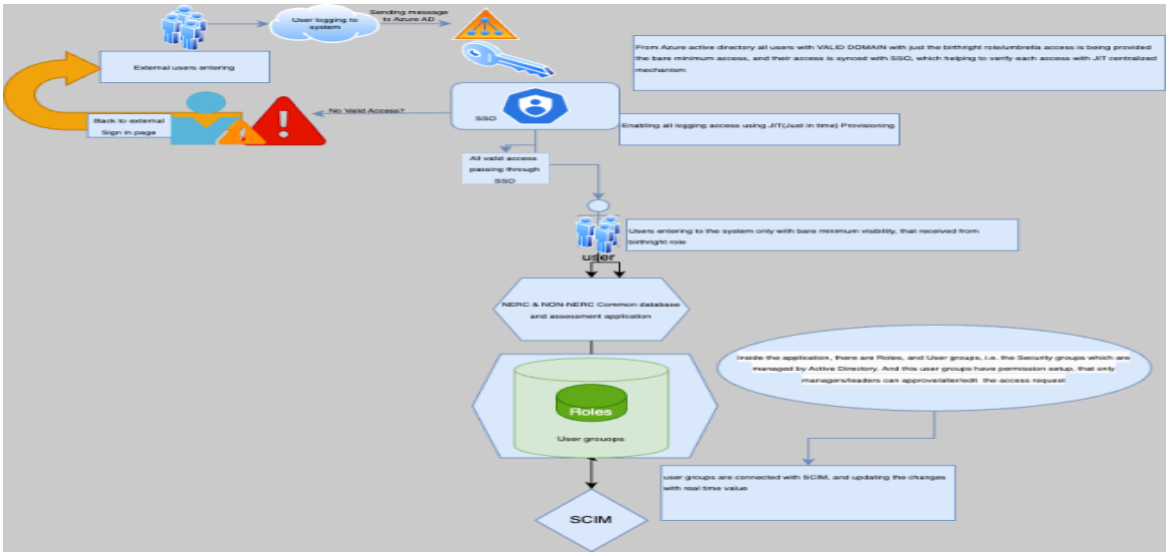

Fig 1: Visual Representation

1. Visual Representation and workflow:

i. Phase 1: Birthright Access and Umbrella Access Step 1: Authentication via Azure AD

- All users, when entering the system, are authenticated through Azure Active Directory (Azure AD).
- They are granted minimal "birthright" access, meaning that all users receive the baseline level of access necessary to interact with the system, regardless of their specific roles.
- This access is synchronized and validated using SSO (Single Sign-On) with a Just-in-Time (JIT) mechanism, which ensures that users' identities are verified before accessing the system.
- At this stage, users only have bare minimum visibility, which is managed through their birthright roles.
- Phase 1 Objective: The first phase grants users the baseline access to the system, allowing them to log in and view basic information based on their initial role, without being able to interact with sensitive data directly.

ii. Phase 2: Granular Role-Based Access and Approval Process

Step 2: Role and User Group Management

- Inside the application, users' roles and user groups are managed by Active Directory, which defines the specific permissions for each role.
- Managers and leaders within the system are given the ability to approve, alter, or modify access requests. This step ensures that only users with specific permissions can escalate their access based on their role and responsibility.

Step 3: SCIM Integration for Granular Access

- SCIM (System for Cross Domain Identity
- Management) plays a critical role in synchronizing and managing user groups at a granular level.
- SCIM ensures that only the users who are part of specific, authorized user groups are granted access to more sensitive or detailed information within the system.

- This phase enables precise access controls, limiting visibility and interaction with NERC-related data to those with the appropriate permissions, based on their roles in the system.
- Phase 2 Objective: The second phase ensures that access to critical data is tightly controlled through granular role-based access management. This phase requires managerial approval for higher-level access and leverages SCIM to manage and synchronize user roles across the system.

2. Bridging High-Level Authentication and Granular Access Control

   The paper highlights the gap between umbrella-level authentication provided by SSO and the need for granular access control in managing NERC data. The diagram demonstrates this clearly:

   - Azure AD with SSO: Shows the baseline authentication process, where all users receive minimal access, ensuring valid domain-level entry into the system.
   - SCIM Integration: Addresses the limitations of SSO by adding role-based and user group-specific access controls, as discussed in the paper's two-phase access model. SCIM ensures that only NERC-certified users can access sensitive repositories, which aligns with the principle of least privilege outlined in the BCSI standards.

3. Aligning with Regulatory and Security Requirements

   The paper emphasizes the importance of compliance with NERC Critical Infrastructure Protection (CIP) standards, particularly BCSI requirements for protecting critical assets. The diagram shows:

   - How the system ensures regulatory alignment by segregating NERC and non-NERC data access through security groups.
   - How roles and permissions are managed dynamically, reducing the risk of unauthorized access, which directly supports the paper's discussion on enforcing compliance in hybrid environments like AWS and Azure.

4. Addressing Hybrid Cloud Challenges The paper discusses the complexity of implementing security frameworks in hybrid environments that include both on-premises and public cloud infrastructures like AWS and Azure. The diagram fits by showcasing:

   - Azure AD's role as a centralized identity provider, syncing users and permissions across hybrid platforms.
   - SCIM’s automation and synchronization processes that handle real-time updates, a critical capability for managing hybrid cloud environments effectively.

III. CONCLUSION

In the modern utility sector, ensuring the security and integrity of sensitive data, especially within systems governed by NERC (North American Electric Reliability Corporation) standards, is paramount. With the increasing digitization of operational and IT infrastructures, including cloud-based environments, robust identity and access management (IAM) solutions are essential to safeguarding critical information. The integration of Single Sign-On (SSO) and System for Cross Domain Identity Management (SCIM) provides a comprehensive and scalable framework for managing user access, ensuring that only authorized personnel can interact with sensitive NERC data.

The two-phase access management model—starting with minimal birthright access and followed by granular, role-based access management—offers a balanced approach to security and user management. In the first phase, the implementation of SSO with a Just-in-Time (JIT) mechanism grants users the basic access required for system navigation, while ensuring that each user’s identity is validated in real-time. In the second phase, SCIM facilitates the synchronization of user groups, allowing for detailed and dynamic access control, where only authorized personnel can access and modify NERC-related data based on managerial approval.

This approach not only meets regulatory requirements but also bridges the gap between complex, large-scale utility operations and practical security implementation. By combining real-time updates with centralized management, the proposed framework enhances the security posture of utility organizations, ensuring compliance with NERC's Critical Infrastructure Protection (CIP) standards while minimizing the risk of unauthorized access.

Ultimately, as the utility industry continues to evolve and embrace new technologies, the need for effective, scalable, and adaptable security solutions will remain critical. By leveraging advanced IAM systems like SSO and SCIM, utilities can ensure that their infrastructures are not only secure but also resilient to the growing range of cyber threats, ensuring the continued reliability of essential services in a digital world.

IV. REFERENCES

[1] Y. Ten, C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems," IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836– 1846, Nov. 2008, doi: 10.1109/TPWRS.2008.2002298.

[2] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," International Journal of Critical Infrastructure Protection, vol. 8, pp. 53–66, Dec. 2015, doi: 10.1016/j.ijcip.2014.12.002.

[3] L. Wang and C. D. Scoggins, "Enhancing security and privacy in the utility sector through SSO and SCIM integration," in Proc. IEEE SmartGridComm, 2019, pp. 1–5, doi: 10.1109/SmartGridComm.2019.8909745.

[4] A. Saleh et al., "Cloud-based cybersecurity for the energy sector: Role of IAM and SSO," IEEE Access, vol. 9, pp. 82156–82169, May 2021, doi: 10.1109/ACCESS.2021.3073156.

[5] North American Electric Reliability Corporation (NERC), "Critical Infrastructure Protection Standards,"NERC Standards, Version 6, 2021. [Online]. Available: https://www.nerc.com

[6] E. Bertino and R. Sandhu, "Database security— concepts, approaches, and challenges," IEEE Transactions on Dependable and Secure Computing,
vol. 2, no. 1, pp. 2– 19, Jan.–Mar. 2005, doi: 10.1109/TDSC.2005.7.

[7] J. Hammer et al., "Access management strategies for hybrid cloud environments," IEEE Cloud Computing, vol. 8, no. 4, pp. 40–49, Jul.–Aug. 2021, doi: 10.1109/MCC.2021.3085625.

[8] P. Samarati, "Access control: Policies, models, and mechanisms," in Foundations of Security Analysis and Design III, Springer, 2005, pp. 137–196.

[9] A. Banafa, "Securing the grid: Emerging technologies in utility cybersecurity," IEEE Internet of Things Magazine, vol. 3, no. 4, pp. 58–62, Dec. 2020, doi: 10.1109/IOTM.2020.3035029.

[10] D. D. Clark and D. R. Wilson, "A comparison of commercial and academic IAM frameworks," Communications of the ACM, vol. 59, no. 7, pp. 78–84,
Jul. 2016, doi: 10.1145/2911982.

[11] A. Chakrabarti and G. Manimaran, "Internet infrastructure security: A taxonomy," IEEE Network, vol. 16, no. 6, pp. 13–21, Nov. 2002, doi: 10.1109/MNET.2002.1045498.

[12] S. Ullah et al., "IAM best practices for energy-critical data protection," IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4281–4292, Jun. 2021, doi: 10.1109/TII.2021.3045441.

[13] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol.
34, no. 1, pp. 1–11, Jan. 2011, doi: 10.1016/j.jnca.2010.07.006.

[14] H. Kim and J. Park, "A security architecture for NERC compliance in the smart grid," Energy Informatics, vol. 4, no. 1, p. 11, 2021, doi: 10.1186/s42162-021-00142-8.

[15] E. Bertino, "Data protection in cloud-based systems: Role of IAM frameworks," ACM Computing Surveys, vol. 51, no. 1, pp. 1–36, Jan. 2018, doi: 10.1145/3152897.

[16] Y. Cheng et al., "Real-time monitoring and auditing in hybrid environments," Future Generation Computer Systems, vol. 108, pp. 1081–1095, Aug. 2020, doi: 10.1016/j.future.2020.02.042.

[17] R. Lu et al., "A lightweight access control framework for hybrid energy systems," IEEE Transactions on Smart Grid, vol. 12, no. 1, pp. 24–34, Jan. 2021, doi: 10.1109/TSG.2020.3015126.

[18] S. Malik, S. U. Rehman, and A. Shafique, "Risk management framework for securing critical infrastructure in the utility sector," IEEE Access, vol. 8, pp. 23451–23466, Feb. 2020, doi: 10.1109/ACCESS.2020.2971224.

[19] Z. Ma et al., "Dynamic role-based access control in cloud environments for critical infrastructure protection," Future Generation Computer Systems, vol.
115, pp. 500– 512, Sep. 2021, doi: 10.1016/j.future.2020.09.043.