International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

A Centralized Authentication and Authorization Framework for Enterprise Security Modernization.

Ankush Gupta

Senior Solution Architect, Bothell (Washington)

Abstract

This paper presents the design and implementation of Telecom's enterprise-wide Authentication and Authorization Initiative, aimed at modernizing identity and access management (IAM) across a large-scale digital ecosystem. The initiative introduced a novel token taxonomy - Software/Application Tokens, People Tokens, and Device Tokens - enabling fine-grained, context-aware access control using RBAC, ABAC, and ReBAC models. A Security Library Framework was developed to centralize API token lifecycle management, incorporating low-code integration for developers and uniform enforcement across distributed systems. The project also included a comprehensive API Security Audit, automation with Terraform for secure provisioning on AWS [3] and Azure [4], and AI-powered threat detection using Google Vertex AI [5]. The outcomes included significant vulnerability reduction, streamlined token governance, measurable improvement in external cybersecurity ratings, and enhanced operational efficiency. This initiative demonstrates the effectiveness of combining cloud-native automation, AI-driven security, and centralized IAM in achieving scalable, resilient enterprise security.

Keywords— Authentication, Authorization, Identity and Access Management (IAM), API Security, Cloud Security, AI-driven Security.

I. INTRODUCTION

Digital transformation requires robust and scalable security frameworks. At Telecom, the growing complexity of customer interactions necessitated modernization of authentication and authorization mechanisms. This work introduces a centralized IAM framework to enhance operational resilience and improve security compliance and presents the methodology, execution, and impact of the initiative, emphasizing its contributions to telecom security innovation.

II. BACKGROUND AND RELATED WORK

Traditional IAM relied on fragmented systems with limited adaptability. Industry standards such as OWASP Top Ten [1] and token-based authentication [1], [2] informed the design of a unified, modernized framework.

III. METHODOLOGY

The initiative classified tokens into Application, People, and Device categories. Fine-grained authorization was enabled through RBAC, ABAC, and ReBAC. A Security Library Framework was developed to standardize token generation, validation, and propagation.

IV. IMPLEMENTATION

Key components included:

1) Security Library Framework: Low-code, centralized API security library.
2) API Security Audit: Identified and remediate vulnerabilities in Metro and Prepaid Business units.
3) AI-Powered Security: Integrated Google Vertex AI [5] for anomaly detection, predictive scoring, and autonomous mitigation.
4) Terraform Automation: Automated secure resource provisioning in AWS [3] and Azure [4].
5) Bug Bounty Integration: Proactively identified and addressed production API vulnerabilities.

V. RESULTS AND IMPACT

Outcomes achieved based on one telecom gaint in USA - Removed 18,495 unnecessary API permissions; Eliminated 265 unused APIs and 200,000 lines of insecure code; Retired 180 legacy repositories; Achieved higher external security ratings (ImmuniWeb [7], BitSight [6]); Reduced manual intervention through AI-enabled automation.

VI. INNOVATION

Key innovations:

1) AI-Driven Threat Detection leveraging Google Vertex AI [5].
2) OWASP-based Audit Automation with standardized templates[1]
3) Audit Automation Using the OWASP Top 10 Framework.
4) Novel Token Taxonomy for scalable IAM.

VII. CONCLUSION

The initiative transformed Telecom's authentication and authorization landscape, combining centralized IAM, AI, and cloud-native automation. This framework enhanced resilience, compliance, and operational efficiency, positioning the enterprises as a leader in telecom security innovation, serving as a blueprint for how telecom operators worldwide can adapt to the escalating challenges of cyber threats in the 5G and cloud-native era. Future work should explore quantum-safe cryptography, deeper adoption of zero-trust architectures, and expanded use of machine learning for predictive threat prevention.

References

1. OWASP Foundation, "OWASP Top Ten Web Application Security Risks," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/
2. National Institute of Standards and Technology (NIST), "Digital Identity Guidelines: NIST Special Publication 800-63-3," NIST, 2017. [Online]. Available: https://pages.nist.gov/800-63-3/
3. Amazon Web Services, "AWS Identity and Access Management Documentation," AWS Documentation, 2024. [Online]. Available: https://docs.aws.amazon.com/iam/
4. Microsoft Corporation, "Microsoft Entra ID (Azure Active Directory)," Microsoft Learn, 2024. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/

5. Google Cloud, “Vertex AI Documentation,” Google Cloud Platform, 2024. [Online]. Available: https://cloud.google.com/vertex-ai/docs
6. BitSight, “BitSight Security Ratings,” BitSight, 2024. [Online]. Available: https://www.bitsight.com/
7. ImmuniWeb, “AI-Powered Application Security Testing,” ImmuniWeb, 2024. [Online]. Available: https://www.immuniweb.com/

Acknowledgements

The author thanks the open academic community and prior research efforts in reinforcement learning and security risk modeling that provided the foundation for this work. Inspiration is drawn from collaborations within the telecom services industry and academic conferences where discussions on ethics, security, and responsible AI continue to shape the direction of applied research. Special acknowledgment is extended to mentors, colleagues, and professional organizations like IEEE and ACM that foster a spirit of innovation and rigor in computational finance.

Author Biography

Ankush Gupta is a Security Specialist in API, Cloud and AI security with expertise in data analytics and enterprise transformation strategy. He has led enterprise-scale initiatives in telecom, retail and financial services, focusing on fairness-aware security systems and operational resilience. His work advances operational efficiency, regulatory security compliance, and ethical responsibility in telecom, retail and financial security services.