The American Journal of Engineering and Technology
ISSN 2689-0984 Volume 08 - 2026

Threat Analysis and Risk Assessment of Federated Authentication Architectures: Securing SSO and MFA Workflows

Kwame Mensah
Department of Data Science and Computational Intelligence, African Institute of Digital Analytics, Accra, Ghana

Ama Owusu
Department of Machine Learning and Data Engineering, African Institute of Digital Analytics, Kumasi, Ghana

Received: 05 June 2026 | Received Revised Version: 15 Jul 2026 | Accepted: 25 Aug 2026 | Published: 01 Sep 2026

Volume 08 Issue 09 2026 | Crossref DOI: 10.37547/tajet/Volume08Issue09-02

Abstract

Federated authentication architectures have become a central mechanism for providing scalable access to distributed applications through Single Sign-On (SSO) and Multi-Factor Authentication (MFA). Their security advantage derives from centralized or delegated identity assurance, but federation also creates complex trust relationships among identity providers, service providers, authentication brokers, clients, and authorization components. Consequently, compromise of one critical component can propagate across multiple relying applications. This research presents a structured threat analysis and risk assessment approach for federated authentication architectures, focusing on SSO and MFA workflows. The methodology combines architectural decomposition, STRIDE-oriented threat identification, workflow-level attack analysis, trust-boundary assessment, likelihood-impact scoring, and control-oriented risk prioritization. Particular attention is given to credential theft, token manipulation, replay, session hijacking, identity-provider compromise, MFA bypass, assertion misuse, privilege escalation, repudiation, and availability attacks. The analytical model emphasizes that MFA does not independently eliminate federation risk because authentication assurance can be undermined at protocol, session, recovery, or trust-management layers. The study also incorporates methodological insights from the supplied literature concerning systematic evaluation, robustness, ensemble reasoning, reproducibility, and decomposition of complex systems. The resulting framework provides a practical basis for identifying high-risk authentication paths and strengthening identity federation through layered controls, continuous monitoring, least privilege, resilient session management, and risk-adaptive MFA.

Keywords: Federated Authentication, Single Sign-On, Multi-Factor Authentication, STRIDE, Threat Modeling, Risk Assessment, Identity Security, Access Control, Authentication Workflows, Cybersecurity.

Cite This Article: Mensah, K., & Owusu, ama. (2026). Threat Analysis and Risk Assessment of Federated Authentication Architectures: Securing SSO and MFA Workflows. The American Journal of Engineering and Technology, 8(09), 8–14. https://doi.org/10.37547/tajet/Volume08Issue09-02

1. Introduction

Modern enterprise applications increasingly operate across heterogeneous infrastructure, cloud platforms, partner environments, and externally hosted services. Federated authentication enables users to authenticate through a trusted identity provider and subsequently access multiple relying applications without independently authenticating to each application. SSO therefore improves usability and administrative efficiency, while MFA increases resistance to attacks that depend solely on compromised passwords. However, federation also transforms authentication from an isolated application function into a distributed security architecture containing multiple trust relationships and security-sensitive exchanges.

The fundamental security problem is that successful authentication at one component may establish authorization consequences across many other components. An attacker who compromises an identity provider, authentication session, federation token, or

recovery mechanism may therefore obtain access beyond the original point of compromise. Ganapathy (2024) emphasizes the importance of systematically modeling attack vectors in federated SSO and MFA systems rather than treating authentication as a single isolated security control. This perspective is particularly important because an authentication architecture can remain vulnerable even when individual components appear secure.

The principal objective of this research is to develop a structured threat and risk assessment model for federated SSO and MFA workflows. The study examines where threats emerge, how they propagate through authentication workflows, which assets and trust boundaries are most important, and how security controls should be prioritized according to risk. The analysis covers identity providers, service providers, federation protocols, authentication tokens or assertions, user sessions, MFA mechanisms, administrative interfaces, and account-recovery processes.

A second objective is to establish a systematic evaluation perspective. Several supplied studies demonstrate the value of evaluating complex computational systems through comparative, systematic, robust, or ensemble-oriented approaches (Avila Cobos et al., 2020; Cai et al., 2022; Jeong et al., 2022). Although these studies address biomedical data analysis rather than cybersecurity, their methodological emphasis is useful for this research: complex systems should not be evaluated through a single observation or isolated component. Instead, security assessment should consider multiple attack paths, conditions, and failure modes.

The significance of this research lies in its workflow-centric approach. Rather than asking only whether MFA is enabled or whether an identity provider is protected, the proposed assessment asks whether the complete authentication chain can withstand manipulation, interception, replay, privilege abuse, and trust compromise.

2. Literature Review

2.1 Federated authentication and threat modeling

Federated authentication creates an architectural relationship in which an identity provider establishes or communicates an authentication decision that a relying service subsequently trusts. SSO extends this model by allowing authentication state to be reused across multiple services. MFA strengthens the authentication stage by requiring additional evidence, but the resulting architecture remains dependent on the integrity of tokens, sessions, endpoints, federation configuration, recovery procedures, and trust relationships.

Ganapathy (2024) provides the most directly relevant foundation among the supplied references by applying STRIDE-based analysis to federated SSO and MFA attack vectors. Its central methodological implication is that authentication security should be examined as an attack surface rather than as a binary property. Threats can occur at different stages of the workflow, including identity verification, federation exchange, session establishment, and subsequent access.

2.2 Systematic evaluation as a methodological foundation

The supplied literature provides several methodological principles that can be transferred conceptually to threat assessment. Avila Cobos et al. (2020) emphasize benchmarking multiple cell-type deconvolution pipelines, while Jeong et al. (2022) conduct systematic evaluation of alternative computational pipelines. The relevant methodological lesson is that complex analytical systems can produce different outcomes depending on the method and conditions under which they are evaluated.

For authentication architecture assessment, this principle suggests that a threat model should not depend on one attack scenario. Instead, authentication workflows should be evaluated against multiple threat categories and attack paths. For example, an architecture may resist direct credential theft but remain vulnerable to session compromise or recovery-channel abuse. Consequently, security evaluation should compare attack paths rather than treating the authentication mechanism as a single homogeneous control.

2.3 Robustness, ensemble reasoning, and decomposition

Cai et al. (2022) examine robust estimation through ensemble deconvolution, while Chu et al. (2022) describe Bayesian integrative analysis across different forms of sequencing data. Again, these works are not security studies, but their methodological concepts support an important security principle: complex systems can be assessed more reliably when multiple evidence sources or analytical dimensions are integrated.

Applied to federated authentication, risk assessment can

combine architectural evidence, trust relationships, protocol behavior, authentication logs, configuration weaknesses, and attack-path analysis. Such integration reduces the possibility that a risk assessment focuses excessively on one visible vulnerability while overlooking a less obvious but more consequential pathway.

Jaffe and Irizarry (2014) demonstrate the importance of accounting for heterogeneity in analytical studies. In a conceptual security parallel, federated authentication environments are also heterogeneous: organizations may employ different identity providers, applications, MFA mechanisms, authorization policies, and administrative practices. A threat model that assumes homogeneous components may therefore underestimate security risk.

2.4 Research gap

The supplied bibliography reveals a substantial gap between the security problem addressed by this research and the majority of the provided literature. Most references investigate biological heterogeneity, deconvolution, methylation, transcriptomics, or statistical modeling (Gasparoni et al., 2018; Luo et al., 2022; Newman et al., 2015; Patrick et al., 2020; Salas et al., 2022). These publications cannot legitimately be interpreted as empirical evidence about SSO or MFA security.

Accordingly, the present research adopts them only as methodological analogies for systematic evaluation, robustness, decomposition, and reproducibility. The direct conceptual security basis is Ganapathy (2024). This distinction is important for research integrity because methodological transfer should not be confused with domain-specific empirical evidence.

3. Methodology

3.1 Research design

This study adopts a structured, architecture-centered threat analysis and risk assessment methodology. The research treats federated authentication as a sequence of interacting security functions rather than as a single authentication event. The workflow is decomposed into identity request, authentication, MFA verification, federation assertion or token issuance, service-provider validation, session creation, authorization, and session termination or recovery.

The approach contains five analytical stages: asset identification, trust-boundary decomposition, STRIDE-oriented threat enumeration, risk scoring, and control prioritization. This structure is consistent with the broader methodological principle of systematic evaluation represented in the supplied literature (Avila Cobos et al., 2020; Jeong et al., 2022).

3.2 Architectural decomposition

The primary assets considered are user credentials, MFA credentials or authenticators, authentication tokens, federation assertions, session identifiers, identity attributes, authorization decisions, administrative credentials, and audit records.

The principal entities are the user, client device, identity provider (IdP), MFA service, federation protocol layer, service provider (SP), authorization system, and administrative plane. Trust boundaries exist between the user and IdP, IdP and SP, client and browser session, federation authority and application, and administrators and identity infrastructure.

This decomposition is essential because an attacker does not necessarily need to compromise the strongest component. A weakness at a less protected boundary can undermine the security guarantees of the entire architecture.

3.3 STRIDE-oriented threat identification

The threat model categorizes risks into spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

Spoofing includes stolen credentials, compromised sessions, fraudulent identity assertions, and attacks that circumvent MFA. A hypothetical example is an attacker acquiring a valid session after MFA completion and subsequently presenting the session as evidence of authentication.

Tampering involves manipulation of authentication assertions, authorization attributes, redirect parameters, session information, or identity claims. The principal risk is that a relying service accepts modified information as trustworthy.

Repudiation concerns insufficient evidence to establish which identity performed a security-sensitive operation. Weak audit trails may make investigation difficult after account compromise.

Information disclosure includes leakage of credentials, tokens, identity attributes, recovery information, and

authentication metadata. Excessive identity information transferred between federated parties can increase the consequences of a compromise.

Denial of service targets identity providers, authentication gateways, MFA infrastructure, or federation dependencies. Because multiple applications may depend on a common identity service, availability attacks against the IdP can produce broad organizational impact.

Elevation of privilege occurs when a valid low-privilege identity obtains administrative or otherwise unauthorized permissions. This can result from manipulated claims, incorrect role mapping, excessive federation trust, compromised administrative accounts, or weaknesses in account recovery.

Ganapathy (2024) provides the principal security-oriented basis for applying STRIDE to federated SSO and MFA attack surfaces.

3.4 MFA-specific workflow analysis

MFA should be analyzed as a workflow rather than merely as an authentication setting. An architecture can require MFA during initial login but provide weaker mechanisms during password recovery, device enrollment, session restoration, or high-risk administrative operations.

For example, an attacker may fail to obtain the victim's MFA factor but exploit an inadequately protected recovery mechanism. Similarly, a stolen authenticated session may allow an attacker to operate without repeatedly triggering MFA. Therefore, MFA assurance depends on the complete lifecycle of identity verification.

The assessment consequently examines five stages: initial authentication, second-factor verification, token issuance, session maintenance, and account recovery. Each stage receives independent threat analysis.

3.5 Risk assessment model

Risk is assessed by combining estimated likelihood and potential impact. A conceptual risk score can be represented as:

Risk = Likelihood × Impact

Likelihood reflects exploitability, exposure, attacker opportunity, and the complexity of the attack path. Impact reflects confidentiality, integrity, availability, and privilege consequences.

A critical weakness in an IdP should generally receive greater attention than an isolated low-privilege application weakness because the IdP can provide access to multiple relying services. This illustrates the importance of considering blast radius rather than only vulnerability severity.

3.6 Control prioritization

Controls are prioritized according to the attack paths they interrupt. Preventive controls include phishing-resistant MFA, credential protection, strong federation configuration, least privilege, secure token validation, administrative separation, and hardened recovery procedures. Detective controls include authentication logging, anomaly detection, session monitoring, and administrative-event auditing. Resilience controls include redundant authentication infrastructure, recovery procedures, and incident-response mechanisms.

The methodological emphasis on robust evaluation found in the supplied literature (Cai et al., 2022) supports assessing controls under multiple conditions rather than assuming that a control is universally effective.

4. Results

The analysis identifies the identity provider as the highest-leverage security component in a federated SSO architecture. Because multiple service providers can rely on the same identity decision, compromise of the IdP can create a disproportionate blast radius. The resulting risk is not limited to credential theft; administrative compromise, malicious configuration changes, fraudulent federation assertions, and manipulation of identity attributes can also affect downstream services. Ganapathy (2024) similarly positions federated SSO and MFA as architectures requiring explicit analysis of interconnected attack vectors rather than isolated authentication controls.

A second finding is that MFA substantially improves authentication resilience but does not eliminate federation risk. MFA protects the authentication stage against many password-only attacks, yet threats can shift toward session theft, token compromise, recovery abuse, endpoint compromise, or social engineering. Therefore, measuring security solely by MFA adoption can create an incomplete risk picture. The relevant security property is the integrity of the entire authentication workflow.

Third, trust boundaries represent major attack surfaces.

Federation requires one system to trust authentication information generated by another system. Consequently, incorrect trust configuration, excessive permissions, weak validation, or compromised metadata can transform a localized weakness into a cross-application security problem. The decomposition principle used in systematic analytical research provides a useful methodological parallel: security evaluation should isolate individual components while also examining their interactions (Jeong et al., 2022).

Fourth, session management becomes a critical post-authentication control. Once a user has successfully completed SSO and MFA, subsequent authorization frequently depends on an active session. A stolen session can therefore undermine the protection provided by the original authentication process. Risk assessment should consequently consider session duration, invalidation, device changes, privilege transitions, and suspicious activity.

Fifth, recovery and administrative workflows can become weaker links than normal login. Organizations frequently concentrate security controls on ordinary authentication while giving less attention to account recovery, device enrollment, emergency access, and privileged administration. These pathways should receive the same threat-modeling rigor as initial authentication.

Finally, the analysis indicates that risk assessment should be systematic and multi-dimensional. The supplied literature repeatedly demonstrates the methodological importance of comparing approaches, accounting for heterogeneity, and evaluating robustness (Avila Cobos et al., 2020; Jaffe & Irizarry, 2014; Cai et al., 2022). Applied to federation, this means assessing multiple attack paths and operational conditions rather than relying on one security indicator.

5. Discussion

The findings reinforce the theoretical position that federated authentication security is an architectural property rather than simply a feature of passwords or MFA. SSO introduces efficiency because one authentication event can support access to multiple applications, but the same concentration of trust creates systemic consequences when a critical identity component is compromised. The resulting trade-off is therefore between centralized identity assurance and concentration of security dependency.

The most important practical implication is that organizations should treat the IdP as a high-value security boundary. Strong administrator authentication, privilege separation, configuration protection, continuous monitoring, and rapid incident response are particularly important because IdP compromise can affect many relying services. Ganapathy (2024) supports this attack-surface perspective by emphasizing structured analysis of federated SSO and MFA threats.

The second implication concerns MFA design. MFA should not be evaluated solely according to whether a second factor exists. Its effective security depends on factor enrollment, recovery, session continuity, device trust, and resistance to bypass. A technically strong factor can still provide limited protection if an attacker can circumvent the surrounding workflow. This finding changes the security objective from “implement MFA” to “preserve authentication assurance throughout the identity lifecycle.”

A further implication concerns interoperability and heterogeneity. Federated environments commonly contain multiple service providers with different security requirements. Methodological work emphasizing systematic evaluation and heterogeneity (Avila Cobos et al., 2020; Jeong et al., 2022) suggests that one generalized security assumption may be inadequate. Each relying application should be assessed for its own trust relationship, authorization mapping, and consequences of identity compromise.

The study also identifies a limitation in the available evidence base. Most of the supplied references are biomedical and computational-statistics studies rather than cybersecurity research. They provide useful methodological concepts but cannot establish empirical claims about SSO or MFA attacks. For that reason, the present work should be regarded primarily as a structured conceptual threat and risk assessment rather than a statistically validated empirical security benchmark.

A second limitation is that risk scores in a conceptual framework depend on organizational context. The likelihood of a phishing attack, the value of an administrative account, and the blast radius of an IdP compromise vary across environments. Therefore, organizations should calibrate risk assessment using their own asset inventories, threat intelligence, authentication logs, and business impact assessments.

Future research should validate the framework using

real-world federation configurations, controlled attack simulations, incident datasets, and comparative evaluation of different MFA and federation architectures. Such empirical work would enable quantitative estimation of attack likelihood and control effectiveness.

6. Conclusion

Federated SSO and MFA architectures provide substantial operational benefits but create interconnected security dependencies that require systematic threat analysis. The assessment presented in this study demonstrates that the principal risks extend beyond password compromise to include identity-provider compromise, assertion manipulation, session theft, recovery abuse, privilege escalation, trust-boundary weaknesses, repudiation, information disclosure, and availability attacks.

The central contribution is a workflow-oriented risk assessment model that combines architectural decomposition, STRIDE-based threat identification, likelihood-impact analysis, and control prioritization. The analysis demonstrates that MFA should be considered one component of a broader authentication assurance chain rather than a complete security solution. Protection must continue across authentication, token issuance, session management, authorization, recovery, and administration.

Methodologically, the supplied literature supports the importance of systematic evaluation, robustness, decomposition, and consideration of heterogeneous environments (Cai et al., 2022; Avila Cobos et al., 2020; Jaffe & Irizarry, 2014). However, because most supplied references concern biomedical computation, they should not be interpreted as direct evidence of cybersecurity behavior. The direct security foundation is therefore the supplied federated SSO/MFA threat-modeling study by Ganapathy (2024).

Future research should extend this conceptual model through empirical attack simulations, real-world authentication telemetry, quantitative risk estimation, and comparative evaluation of federation and MFA implementations. Such research can strengthen the transition from qualitative threat modeling toward measurable, adaptive, and continuously updated identity-security risk management.

References

1. Altboum Z, Steuerman Y, David E, Barnett-Itzhaki Z, Valadarsky L, Keren-Shaul H, et al. (2014). Digital cell quantification identifies global immune cell dynamics during influenza infection. Molecular Systems Biology, 10: 720. https://doi.org/10.1002/msb.134947
2. Avila Cobos F, Alquicira-Hernandez J, Powell JE, Mestdagh P, De Preter K (2020). Benchmarking of cell type deconvolution pipelines for transcriptomics data. Nature Communications, 11: 1–14. https://doi.org/10.1038/s41467-019-13993-7
3. Cai M, Yue M, Chen T, Liu J, Forno E, Lu X, et al. (2022). Robust and accurate estimation of cellular fraction from tissue omics data via ensemble deconvolution. Bioinformatics, 38: 3004–3010. https://doi.org/10.1093/bioinformatics/btac279
4. Cai M, Zhou J, McKennan C, Wang J (2024). scmd facilitates cell type deconvolution using single-cell dna methylation references. Communications Biology, 7: 1. https://doi.org/10.1038/s42003-023-05690-5
5. Chang W, Wan C, Lu X, Tu S-w, Sun Y, Zhang X, et al. (2019). Ictd: A semi-supervised cell type identification and deconvolution method for multi-omics data. bioRxiv preprint: https://doi.org/10.1101/426593.
6. Chen W, Wang T, Pino-Yanes M, Forno E, Liang L, Yan Q, et al. (2017). An epigenome-wide association study of total serum ige in hispanic children. Journal of Allergy and Clinical Immunology, 140: 571–577. https://doi.org/10.1016/j.jaci.2016.11.030
7. Chu T, Wang Z, Pe'er D, Danko CG (2022). Cell type and gene expression deconvolution with bayesprism enables bayesian integrative analysis across bulk and single-cell rna sequencing in oncology. Nature Cancer, 3: 505–517. https://doi.org/10.1038/s43018-022-00356-3
8. Gasparoni G, Bultmann S, Lutsik P, Kraus TF, Sordon S, Vlcek J, et al. (2018). Dna methylation analysis on purified neurons and glia dissects age and alzheimer's disease-specific changes in the human cortex. Epigenetics & Chromatin, 11: 1–19. https://doi.org/10.1186/s13072-017-0171-z
9. Guintivano J, Aryee MJ, Kaminsky ZA (2013). A cell epigenotype specific model for the correction of brain cellular heterogeneity bias and its application to age, brain region and major depression. Epigenetics, 8: 290–302. https://doi.org/10.4161/epi.23924
10. Jaffe AE, Irizarry RA (2014). Accounting for cellular heterogeneity is critical in epigenome-wide

association studies. Genome Biology, 15: R31. https://doi.org/10.1186/gb-2014-15-2-r31

11. Jeong Y, de Andrade e Sousa LB, Thalmeier D, Toth R, Ganslmeier M, Breuer K, et al. (2022). Systematic evaluation of cell-type deconvolution pipelines for sequencing-based bulk dna methylomes. Briefings in Bioinformatics, 23: bbac248. https://doi.org/10.1093/bib/bbac248
12. Jiang Y, Gruzieva O, Wang T, Forno E, Boutaoui N, Sun T, et al. (2019). Transcriptomics of atopy and atopic asthma in white blood cells from children and adolescents. European Respiratory Journal, 53: 1900102.
13. Lawrence I, Lin K (1989). A concordance correlation coefficient to evaluate reproducibility. Biometrics, 45: 255–268.
14. Luo C, Liu H, Xie F, Armand EJ, Siletti K, Bakken TE, et al. (2022). Single nucleus multi-omics identifies human cortical cell regulatory genome diversity. Cell genomics, 2: 100107. https://doi.org/10.1016/j.xgen.2022.100107
15. Newman AM, Liu CL, Green MR, Gentles AJ, Feng W, Xu Y, et al. (2015). Robust enumeration of cell subsets from tissue expression profiles. Nature Methods, 12: 453–457. https://doi.org/10.1038/nmeth.3337
16. Patrick E, Taga M, Ergun A, Ng B, Casazza W, Cimpean M, et al. (2020). Deconvolving the contributions of cell-type heterogeneity on cortical gene expression. PLOS Computational Biology, 16: e1008120. https://doi.org/10.1371/journal.pcbi.1008120
17. Psioda MA (2016). Statistical methods for Bayesian clinical trial design and DNA methylation deconvolution, PhD thesis, The University of North Carolina at Chapel Hill.
18. Racle J, de Jonge K, Baumgaertner P, Speiser DE, Gfeller D (2017). Simultaneous enumeration of cancer and immune cell types from bulk tumor gene expression data. eLife, 6: e26476. https://doi.org/10.7554/eLife.26476
19. Salas LA, Zhang Z, Koestler DC, Butler RA, Hansen HM, Molinaro AM, et al. (2022). Enhanced cell deconvolution of peripheral blood using dna methylation for high-resolution immune profiling. Nature Communications, 13: 761.
20. Swapna LS, Huang M, Li Y (2023). Gtm-decon: Guided-topic modeling of single-cell transcriptomes enables sub-cell-type and disease-subtype deconvolution of bulk transcriptomes. Genome Biology, 24: 190. https://doi.org/10.1186/s13059-023-03034-4
21. Teschendorff AE, Zhu T, Breeze CE, Beck S (2020). Episcore: Cell type deconvolution of bulk tissue DNA methylomes from single-cell RNA-seq data. Genome Biology, 21: 1–33. https://doi.org/10.1186/s13059-019-1906-x
22. Zhang Z, Wiencke JK, Kelsey KT, Koestler DC, Molinaro AM, Pike SC, et al. (2023). Hierarchical deconvolution for extensive cell type resolution in the human brain using dna methylation. Frontiers in Neuroscience, 17: 1198243. https://doi.org/10.3389/fnins.2023.1198243
23. Zheng X, Zhang N, Wu H-J, Wu H (2017). Estimating and accounting for tumor purity in the analysis of dna methylation data from cancer studies. Genome Biology, 18: 17.
24. Zhu L, Lei J, Devlin B, Roeder K (2018). A unified statistical framework for single cell and bulk rna sequencing data. Annals of Applied Statistics, 12: 609.
25. Ganapathy, S. K. (2024). Threat Modeling for Federated SSO and MFA Systems: STRIDE-Based Analysis of Attack Vectors. International Journal of Data Science and Machine Learning, 4(02), 55-73. https://www.academicpublishers.org/journals/index.php/ijdsml/article/view/stride-analysis-sso-mfa