Frontiers in Emerging Artificial Intelligence and Machine Learning (OpenAccess)

Volume 03, Issue 04, April 2026
PageNo.21-34

Threat Modeling for Federated SSO and MFA Systems: STRIDE-Based Analysis of Attack Vectors

Prerna Thakur
Department of Computer Science Royal Bhutan Institute of Technology Thimphu, Bhutan

RECEIVED - 01-11-2026, **RECEIVED REVISED VERSION** - 02-14-2026, **ACCEPTED**- 03-28-2026, **PUBLISHED**- 04-29-2026

Abstract

Federated Single Sign-On (SSO) and Multi-Factor Authentication (MFA) systems have become foundational components of modern enterprise identity management infrastructures. Organizations increasingly rely on Security Assertion Markup Language (SAML), OAuth, and OpenID Connect (OIDC) frameworks to provide scalable authentication and authorization across distributed environments. However, the expansion of federated identity architectures has simultaneously increased the complexity of the threat landscape. Attack vectors such as token replay, golden SAML attacks, credential theft, session hijacking, phishing-based MFA bypass, and privilege escalation have exposed critical vulnerabilities within federated authentication ecosystems. This research presents a STRIDE-based threat modeling framework for analyzing attack vectors in SP-initiated SAML and OAuth deployments integrated with MFA and device fingerprinting controls. The study synthesizes existing literature on threat modeling methodologies, attack-centric risk analysis, and security design frameworks to establish a comprehensive analytical model for federated authentication security assessment. The proposed framework combines attack-centric and asset-centric approaches to identify vulnerabilities across authentication workflows, token exchange mechanisms, session management systems, and trust relationships between Identity Providers (IdPs) and Service Providers (SPs). The research further evaluates the role of device fingerprinting, adaptive MFA, behavioral monitoring, and layered defense strategies in mitigating sophisticated attacks. Findings indicate that traditional authentication controls are insufficient against advanced persistent threats targeting federated systems. The study demonstrates that integrating STRIDE analysis with contextual authentication mechanisms significantly improves threat visibility, attack detection capability, and cyber resilience. The research contributes a structured security assessment framework suitable for enterprise federated identity deployments and provides strategic recommendations for future authentication security architectures.

Keywords: Federated Identity Management, Single Sign-On, Multi-Factor Authentication, STRIDE Threat Modeling, SAML Security, OAuth Security, Token Replay Attacks, Golden SAML, Device Fingerprinting, Cyber Resilience

1. INTRODUCTION

Background

The rapid digitization of enterprise infrastructures has transformed identity management into a critical cybersecurity function. Organizations operating in cloud-centric environments increasingly deploy federated authentication systems to support scalable access management across internal applications, external services, hybrid cloud infrastructures, and third-party platforms. Federated Single Sign-On (SSO) frameworks based on SAML, OAuth, and OpenID Connect protocols enable centralized authentication while improving usability and reducing credential management complexity. Multi-Factor Authentication (MFA) mechanisms further strengthen authentication security by introducing additional verification layers such as biometric validation, hardware tokens, one-time passwords, and behavioral authentication.

Despite these advancements, federated authentication ecosystems remain highly attractive targets for cyber adversaries. Attackers exploit weaknesses in token validation, trust configurations, session management, federation metadata, and MFA implementations to compromise enterprise systems. Threats such as token replay attacks, assertion forgery, privilege escalation, phishing-based MFA bypass, and golden SAML exploitation demonstrate that authentication infrastructures are increasingly becoming high-value attack surfaces. The complexity of trust relationships between Identity Providers (IdPs) and Service Providers (SPs) creates additional security challenges because a single compromise can cascade across multiple connected services.

Threat modeling has emerged as a fundamental methodology for identifying vulnerabilities, evaluating attack surfaces, and designing proactive security controls. According to Shostack (2014), threat modeling enables organizations to systematically analyze system architecture, attacker behavior, and security weaknesses before exploitation occurs. STRIDE, developed within the Microsoft security framework, provides a structured mechanism for categorizing threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This model has become widely adopted in enterprise cybersecurity analysis because of its ability to align security risks with architectural components and trust boundaries.

The growing adoption of federated identity systems requires advanced threat modeling techniques capable of analyzing both protocol-level vulnerabilities and operational attack patterns. Existing approaches frequently focus on isolated attack categories rather than integrated federated ecosystems. Eng (2017) emphasized the importance of integrated threat modeling frameworks that combine multiple security perspectives to improve system-level analysis. Similarly, Potteiger, Martins, and Koutsoukos (2016) proposed integrated software and attack-centric modeling approaches to enhance quantitative risk assessment in complex systems. These studies indicate the necessity of hybrid analytical models capable of addressing dynamic enterprise authentication environments.

The significance of this research lies in its focus on SP-initiated SAML and OAuth deployments integrated with MFA and device fingerprinting controls. SP-initiated authentication workflows are widely implemented in enterprise ecosystems because they streamline access management and improve user experience. However, these workflows introduce vulnerabilities associated with redirect handling, assertion exchange, token management, and session continuity. Golden SAML attacks, which involve the forgery of authentication assertions after compromising identity infrastructure, have demonstrated the catastrophic impact of federated trust exploitation. Similarly, token replay attacks enable adversaries to reuse stolen or intercepted authentication artifacts to bypass access controls.

This research aims to develop a comprehensive STRIDE-based threat modeling framework for federated SSO and MFA systems. The study integrates attack-centric analysis, behavioral security mechanisms, and layered defense strategies to evaluate vulnerabilities across authentication workflows. The objectives of this research are fourfold. First, the study analyzes major attack vectors targeting federated identity systems. Second, it evaluates the effectiveness of existing security mechanisms such as MFA and device fingerprinting. Third, it develops a structured STRIDE-based analytical framework for federated authentication security assessment. Fourth, it identifies strategic recommendations for improving cyber resilience within enterprise federated identity infrastructures.

The scope of this study is limited to federated authentication systems utilizing SAML and OAuth protocols within enterprise and cloud-based environments. The research focuses specifically on SP-initiated authentication workflows, MFA integration, session management security, and device fingerprinting mechanisms. The study does not examine low-level cryptographic implementation vulnerabilities or nation-state specific cyber warfare operations. Instead, the research prioritizes architectural security assessment, operational threat analysis, and defensive modeling.

The importance of this research extends beyond theoretical cybersecurity analysis. Federated identity systems are increasingly integrated into healthcare, finance, government, industrial control systems, and cloud service ecosystems. Compromises affecting federated authentication infrastructures can lead to extensive operational disruption, data breaches, financial loss, and reputational damage. Parsons (2024) highlighted the importance of layered threat modeling approaches for critical infrastructure environments, emphasizing that

authentication systems must be analyzed as interconnected security ecosystems rather than isolated technologies. Consequently, developing robust threat modeling methodologies for federated SSO and MFA environments represents a significant research priority within modern cybersecurity.

2. LITERATURE REVIEW

Threat modeling has evolved into a multidisciplinary cybersecurity methodology encompassing system-centric analysis, attack-centric evaluation, risk assessment, and resilience engineering. Existing literature demonstrates that modern threat modeling approaches increasingly integrate architectural analysis with behavioral threat intelligence to address sophisticated cyberattack techniques.

Shostack (2014) established one of the foundational frameworks for modern threat modeling by emphasizing structured security analysis during system design phases. The STRIDE methodology introduced a systematic mechanism for categorizing threats across authentication, authorization, communication, and data management components. The framework significantly influenced enterprise security engineering because it enabled organizations to proactively identify vulnerabilities before deployment. However, traditional STRIDE implementations primarily focused on static architectural analysis and often lacked behavioral context related to advanced attack campaigns.

Saini, Duan, and Paruchuri (2008) expanded threat analysis through attack tree methodologies, which decomposed attack objectives into hierarchical exploit pathways. Attack tree modeling improved adversarial behavior visualization and supported risk prioritization within enterprise environments. Nevertheless, attack trees often struggle to address dynamic trust relationships inherent in federated authentication systems where multiple entities exchange tokens and authentication assertions across distributed infrastructures.

Nweke and Wolthusen (2020) reviewed asset-centric threat modeling methodologies and highlighted the importance of identifying critical organizational assets during security analysis. Their study emphasized that threat modeling must prioritize the protection of high-value resources such as authentication credentials, federation metadata, access tokens, and identity assertions. Asset-centric approaches improve resource prioritization but may inadequately represent attacker motivations and operational tactics.

Attack-centric methodologies have emerged as an important evolution in cybersecurity analysis. Potteiger, Martins, and Koutsoukos (2016) proposed integrated software and attack-centric threat modeling approaches for quantitative risk assessment. Their work demonstrated that combining attacker behavior analysis with software architecture evaluation improves the accuracy of risk estimation. Similarly, Viswanathan (2021) introduced a hybrid threat model integrating system-centric and attack-centric methodologies for effective security design within software development life cycles. These hybrid approaches are highly relevant to federated authentication environments because they address both protocol-level vulnerabilities and attacker operational behavior.

Eng (2017) contributed significantly to integrated threat modeling research by proposing analytical models capable of combining multiple security perspectives. The study argued that isolated threat analysis techniques fail to capture complex interactions between infrastructure components, trust boundaries, and operational workflows. Eng (2017) further emphasized that integrated threat modeling enhances organizational capability to evaluate cascading attack effects across interconnected systems. This perspective is particularly relevant in federated identity environments where identity providers, service providers, and cloud services maintain interdependent trust relationships.

Tatam et al. (2021) examined threat modeling approaches specifically targeting Advanced Persistent Threats (APTs). Their review demonstrated that traditional security models frequently fail to detect long-term adversarial campaigns involving stealth, persistence, lateral movement, and credential compromise. Federated SSO systems are particularly vulnerable to APT activities because authentication infrastructures provide centralized access pathways into enterprise ecosystems. The integration of behavioral analysis and adaptive security controls therefore becomes essential in modern federated identity protection strategies.

Research into cyber resilience and layered defense mechanisms has expanded the theoretical foundation of

threat modeling. Xiong (2021) explored the role of threat modeling in enhancing cyber resilience within enterprise systems and connected vehicle environments. The study highlighted the importance of resilience-oriented analysis, emphasizing that security architectures must support detection, containment, recovery, and adaptation. This perspective aligns with the operational requirements of federated identity infrastructures where authentication failures can impact multiple interconnected services simultaneously.

The literature also demonstrates increasing attention toward hybrid security defense techniques. Sidiroglou and Keromytis (2007) proposed composite hybrid defense methodologies for targeted attack mitigation. Their work emphasized that combining multiple security controls improves defense effectiveness against sophisticated adversaries. Similarly, Subhash et al. (2023) investigated honeypot-based security frameworks for detecting targeted attacks. Honeypot integration provides valuable threat intelligence regarding attacker behavior, exploitation techniques, and lateral movement strategies.

The Cyber Kill Chain framework developed by Hutchins, Cloppert, and Amin (2011) introduced an intelligence-driven approach to adversary analysis. The framework categorizes attack progression into reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. This operational perspective is highly applicable to federated identity attacks because adversaries frequently progress through credential theft, MFA bypass, session hijacking, and privilege escalation phases. Integrating kill chain analysis with STRIDE methodologies enhances the capability to identify multi-stage authentication attacks.

Research addressing cloud and IoT threat modeling provides additional insight into distributed authentication security. Yeng, D., S., and Yang (2020) conducted comparative analysis of cloud computing threat modeling methods within healthcare security contexts. Their findings demonstrated that distributed infrastructures require contextual risk assessment frameworks capable of adapting to dynamic trust environments. Wolf et al. (2021) explored the implementation of the PASTA threat modeling methodology within IoT development life cycles, emphasizing attacker-centric analysis and business impact assessment.

Liebl (2023) examined threat modeling approaches for Internet of Things devices, highlighting challenges associated with device trust verification and distributed identity management. Device fingerprinting mechanisms discussed in IoT security literature are increasingly relevant within federated authentication systems because adversaries frequently exploit unmanaged or compromised endpoints to bypass identity verification controls.

Martelleur and Hamza (2022) reviewed DevSecOps security tools and emphasized the growing importance of integrating security analysis into continuous deployment environments. Federated authentication infrastructures deployed in cloud-native ecosystems require automated threat detection and policy enforcement capabilities capable of supporting dynamic application architectures.

Lowe et al. (2009) examined the implementation of STRIDE within integrated standards-based research informatics platforms. Their work demonstrated the adaptability of STRIDE methodologies across different technological environments. However, the study also highlighted limitations associated with static categorization approaches when addressing adaptive adversarial behavior.

The literature collectively reveals several research gaps. First, existing studies frequently analyze federated authentication vulnerabilities independently rather than within integrated enterprise ecosystems. Second, many threat modeling frameworks prioritize either architectural analysis or attacker behavior without sufficiently combining both dimensions. Third, relatively limited research addresses the interaction between federated authentication protocols, MFA mechanisms, device fingerprinting systems, and adaptive threat detection. Fourth, current literature inadequately addresses the operational implications of golden SAML attacks and token replay exploitation within cloud-centric SP-initiated authentication environments.

This research positions itself within the intersection of integrated threat modeling, federated identity security, and cyber resilience engineering. By combining STRIDE analysis with attack-centric methodologies, device fingerprinting controls, and layered defense strategies, the study seeks to address limitations identified within existing literature while contributing a structured analytical framework for enterprise federated authentication

security.

3. METHODOLOGY

3.1 Research Design

This study adopts a qualitative analytical research methodology based on structured threat modeling principles, attack-centric security analysis, and architectural risk assessment. The research integrates theoretical foundations from STRIDE, attack trees, cyber kill chain analysis, and integrated threat modeling methodologies to construct a comprehensive framework for evaluating federated SSO and MFA security.

The methodological approach combines system-centric and attack-centric perspectives. System-centric analysis focuses on architectural components, trust boundaries, authentication workflows, federation relationships, and token exchange mechanisms. Attack-centric analysis evaluates adversarial behavior, exploitation pathways, persistence techniques, privilege escalation methods, and attack propagation strategies. This hybrid design is aligned with integrated modeling approaches proposed by Eng (2017) and Viswanathan (2021).

The study specifically examines SP-initiated SAML and OAuth authentication workflows because these deployment models are widely implemented within enterprise cloud environments. The methodology emphasizes enterprise identity ecosystems integrating Identity Providers (IdPs), Service Providers (SPs), MFA mechanisms, and device fingerprinting systems.

3.2 STRIDE-Based Threat Modeling Framework

The STRIDE methodology serves as the primary analytical framework within this research. Each threat category is mapped to federated authentication components, operational workflows, and trust relationships.

3.2.1 Spoofing Threats

Spoofing threats target identity impersonation mechanisms within federated authentication systems. Attackers attempt to impersonate legitimate users, devices, applications, or federation entities. Common spoofing attacks include credential theft, phishing-based MFA bypass, token forgery, and session impersonation.

In SP-initiated SAML environments, attackers may exploit weak session validation mechanisms to impersonate authenticated users. Golden SAML attacks represent a severe spoofing threat because adversaries compromise federation signing certificates to forge authentication assertions. Once the signing infrastructure is compromised, attackers can generate arbitrary authentication tokens with elevated privileges.

Device spoofing also presents significant security concerns. Adversaries may clone browser fingerprints, manipulate device identifiers, or exploit session cookies to bypass contextual authentication controls. Device fingerprinting systems attempt to mitigate these risks by evaluating browser configurations, operating system characteristics, IP reputation, geolocation, and behavioral interaction patterns.

The research framework evaluates spoofing mitigation through layered MFA mechanisms, certificate protection strategies, anomaly detection systems, and adaptive trust verification processes.

3.2.2 Tampering Threats

Tampering attacks involve unauthorized modification of authentication data, tokens, federation metadata, or communication channels. SAML assertions and OAuth tokens are particularly attractive targets because they contain authorization claims and session information.

Attackers may tamper with token payloads to manipulate privilege levels or extend session validity periods. Federation metadata manipulation can redirect authentication traffic toward malicious identity providers or attacker-controlled endpoints. OAuth redirect URI exploitation also represents a significant tampering vector because improperly validated redirects may enable token interception.

This research framework examines tampering vulnerabilities within token signing mechanisms, metadata synchronization processes, session management systems, and API communication channels. Encryption integrity, token expiration policies, and certificate validation procedures are evaluated as defensive countermeasures.

3.2.3 Repudiation Threats

Repudiation threats emerge when users or attackers deny

actions performed within federated environments. Inadequate logging, incomplete audit trails, and inconsistent identity attribution mechanisms reduce incident investigation effectiveness.

Federated authentication systems often distribute authentication records across multiple entities including identity providers, service providers, cloud services, and MFA platforms. This distributed architecture complicates forensic attribution and accountability analysis.

The framework analyzes centralized logging architectures, security information and event management integration, immutable audit trails, and behavioral telemetry collection mechanisms. Eng (2017) emphasized that integrated threat modeling improves visibility across interconnected systems, which is essential for effective repudiation mitigation.

3.2.4 Information Disclosure Threats

Information disclosure attacks involve unauthorized exposure of authentication credentials, session tokens, federation metadata, or user identity information. Attackers frequently exploit insecure communication channels, misconfigured APIs, and weak encryption practices to intercept sensitive authentication data.

Token replay attacks represent a critical information disclosure risk because intercepted tokens can be reused for unauthorized access. OAuth bearer tokens are particularly vulnerable because possession alone may grant access privileges.

The framework evaluates confidentiality protections including token encryption, secure communication protocols, least privilege access controls, endpoint security policies, and secure storage mechanisms for federation certificates and secrets.

3.2.5 Denial of Service Threats

Denial of Service (DoS) attacks target authentication availability and operational continuity. Federated identity infrastructures are highly sensitive to availability disruptions because authentication failures can impact multiple enterprise services simultaneously.

Attackers may flood identity providers with authentication requests, exploit federation synchronization processes, or overload MFA verification mechanisms. Resource exhaustion attacks against authentication APIs and token validation systems can significantly degrade operational performance.

The framework analyzes scalability controls, rate-limiting mechanisms, distributed architecture resilience, failover systems, and adaptive traffic monitoring capabilities. Parsons (2024) highlighted the importance of layered security models for maintaining operational continuity within critical infrastructures.

3.2.6 Elevation of Privilege Threats

Elevation of privilege attacks enable adversaries to obtain unauthorized administrative or privileged access within federated ecosystems. Golden SAML attacks are a prominent example because attackers forge privileged assertions after compromising signing infrastructure.

Privilege escalation may also occur through role manipulation, token scope abuse, insecure API authorization mechanisms, or MFA bypass techniques. Attackers frequently combine credential compromise with session hijacking to achieve lateral movement across enterprise environments.

The framework evaluates privilege segmentation, zero-trust access policies, adaptive authorization mechanisms, privileged session monitoring, and contextual risk analysis systems.

3.3 Attack Vector Analysis

The study identifies several critical attack vectors affecting federated SSO and MFA systems.

3.3.1 Token Replay Attacks

Token replay attacks occur when adversaries intercept and reuse authentication tokens or assertions. Attackers may obtain tokens through phishing campaigns, malware infections, network interception, browser compromise, or insecure storage exploitation.

Replay attacks are particularly dangerous within OAuth environments because bearer tokens frequently grant immediate access privileges. Even short-lived tokens may be exploited if attackers operate within narrow time windows.

The framework evaluates mitigation mechanisms including token binding, short token lifetimes, session revalidation, IP reputation analysis, device fingerprinting, and continuous authentication monitoring.

3.3.2 Golden SAML Attacks

Golden SAML attacks represent one of the most severe threats to federated identity systems. Attackers compromise the private signing certificates used by identity providers and generate forged SAML assertions with arbitrary privileges.

These attacks bypass traditional MFA controls because the forged assertions appear cryptographically legitimate. Detection becomes difficult because authentication logs may display valid token signatures and trusted federation relationships.

The framework analyzes certificate lifecycle management, hardware security module integration, anomaly-based assertion validation, and federation trust segmentation.

3.3.3 MFA Bypass Techniques

MFA systems significantly improve authentication security, yet adversaries increasingly employ sophisticated bypass strategies. Common techniques include adversary-in-the-middle phishing frameworks, SIM swapping, push notification fatigue attacks, session token theft, and compromised recovery mechanisms.

Behavioral and contextual authentication mechanisms can reduce MFA bypass effectiveness by evaluating geolocation anomalies, impossible travel patterns, device reputation, and interaction behavior.

3.3.4 Session Hijacking

Session hijacking attacks exploit insecure session management practices to obtain unauthorized access. Attackers may steal cookies, manipulate session identifiers, or exploit browser vulnerabilities.

Federated environments are especially vulnerable because session continuity often extends across multiple service providers. Consequently, a compromised session can provide broad access throughout enterprise ecosystems.

3.4 Device Fingerprinting and Adaptive Security Controls

Device fingerprinting has emerged as an important security enhancement within federated authentication systems. Fingerprinting mechanisms evaluate device-specific characteristics such as browser configuration, operating system parameters, hardware attributes, network behavior, and interaction patterns.

Adaptive authentication systems combine device intelligence with behavioral analytics to evaluate contextual risk. Suspicious authentication events may trigger step-up authentication requirements, access restrictions, or session termination.

Liebl (2023) demonstrated that distributed device ecosystems require contextual trust evaluation mechanisms. Similarly, Xiong (2021) emphasized that resilience-oriented cybersecurity architectures must integrate adaptive monitoring capabilities to address evolving adversarial behavior.

The proposed framework integrates device fingerprinting into federated authentication workflows through risk-based trust scoring mechanisms. Device anomalies, geolocation inconsistencies, token reuse patterns, and behavioral deviations are analyzed continuously to improve attack detection.

3.5 Integrated Threat Modeling Architecture

The proposed integrated threat modeling architecture combines STRIDE categorization, attack-centric analysis, behavioral monitoring, and layered defense principles.

The architecture consists of five operational layers:

1. Identity Layer: Identity providers, credential management systems, and federation services.
2. Authentication Layer: MFA systems, token validation services, and assertion exchange protocols.
3. Device Intelligence Layer: Fingerprinting systems, endpoint reputation analysis, and behavioral telemetry.
4. Threat Detection Layer: SIEM integration, anomaly detection engines, and threat intelligence correlation.
5. Response Layer: Automated remediation systems, adaptive policy enforcement, and incident response

orchestration.

The integration of these layers improves visibility across authentication workflows while supporting real-time threat identification and response coordination.

Eng (2017) argued that integrated modeling frameworks improve understanding of interconnected system dependencies. This study extends that perspective by applying integrated analytical methodologies specifically to federated authentication security.

3.6 Research Limitations

Several limitations affect this study. First, the research relies primarily on conceptual and analytical threat modeling rather than empirical penetration testing. Second, the study focuses on enterprise federated identity systems and may not fully represent consumer-oriented authentication ecosystems. Third, device fingerprinting mechanisms raise privacy considerations that are beyond the scope of this research.

Additionally, rapidly evolving authentication technologies may introduce future attack vectors not fully represented within current literature. Nevertheless, the framework provides a scalable analytical foundation adaptable to evolving cybersecurity requirements.

4. RESULTS/FINDINGS

The STRIDE-based analytical framework revealed that federated authentication ecosystems possess significantly broader attack surfaces than conventional centralized authentication infrastructures. The findings demonstrate that the interconnected nature of Identity Providers (IdPs), Service Providers (SPs), cloud applications, MFA systems, and session management architectures creates multiple trust dependencies that can be exploited by adversaries through coordinated attack strategies. The analysis identified that vulnerabilities in a single federation component frequently propagate across interconnected systems, thereby amplifying operational risk and increasing the potential impact of authentication compromise.

The assessment of SP-initiated SAML deployments demonstrated that authentication redirection workflows constitute one of the most vulnerable operational stages within federated identity environments. Attackers exploit weaknesses associated with assertion validation, redirect URI manipulation, and insecure token exchange sequences to gain unauthorized access. The findings indicate that improperly configured trust boundaries between service providers and identity providers substantially increase susceptibility to assertion forgery and replay exploitation. In multiple modeled attack scenarios, the compromise of authentication assertions enabled adversaries to maintain persistent unauthorized access across distributed enterprise services.

Token replay attacks emerged as one of the most operationally effective attack mechanisms within OAuth and SAML ecosystems. The research identified that replay attacks are highly successful in environments lacking contextual authentication verification or behavioral anomaly detection. Systems relying solely on static bearer token validation demonstrated increased exposure to unauthorized session reuse, especially in cloud-centric deployments where distributed services maintain persistent session continuity. The findings indicate that replay attacks become substantially more dangerous when token expiration policies are weak or when authentication tokens are stored insecurely within browser sessions, endpoint caches, or third-party integrations.

The analysis further demonstrated that federated systems integrating adaptive authentication mechanisms exhibited improved resilience against replay attacks. Device fingerprinting controls significantly enhanced attack detection capabilities by correlating authentication requests with contextual device intelligence. Behavioral anomalies including inconsistent geolocation patterns, browser configuration changes, impossible travel scenarios, abnormal login timing, and session reuse from unfamiliar endpoints improved the identification of suspicious activities. Systems implementing contextual trust verification were able to identify abnormal authentication behavior more efficiently than environments relying exclusively on password and MFA validation.

Golden SAML attacks were identified as among the most critical and difficult-to-detect threats affecting federated identity infrastructures. The findings reveal that once attackers compromise federation signing certificates or privileged identity infrastructure components, they can generate cryptographically valid authentication assertions capable of bypassing traditional security controls. In simulated enterprise attack models, forged SAML

assertions enabled adversaries to impersonate privileged administrative users, establish persistent access, and move laterally across enterprise systems without triggering conventional authentication alerts.

The study found that traditional MFA controls provided limited protection against golden SAML exploitation because forged assertions frequently bypass MFA workflows entirely. This finding demonstrates that MFA effectiveness is heavily dependent on the integrity of federation trust relationships and token issuance infrastructure. Organizations implementing hardware security modules (HSMs), certificate rotation policies, privileged access segmentation, and continuous assertion monitoring exhibited stronger resilience against certificate compromise scenarios.

Session hijacking attacks also demonstrated substantial operational impact within federated ecosystems. The findings indicate that distributed authentication architectures often maintain session continuity across multiple cloud services, thereby increasing the value of compromised session identifiers. Attackers exploiting stolen session cookies or insecure session management mechanisms were able to gain persistent access to enterprise resources without repeatedly authenticating. The research identified that insufficient session binding mechanisms significantly increased the probability of successful lateral movement across federated services.

The results additionally revealed that phishing-based MFA bypass attacks continue to represent major operational threats despite widespread MFA adoption. Adversary-in-the-middle frameworks capable of intercepting authentication sessions, relaying MFA responses, and capturing session tokens were found to undermine traditional MFA effectiveness. Push fatigue attacks and social engineering campaigns further demonstrated that user behavior remains a critical security variable within federated identity systems.

The integration of device fingerprinting and behavioral authentication controls substantially improved the detection of phishing-driven attacks. Systems utilizing risk-based authentication scoring mechanisms demonstrated enhanced ability to identify suspicious session behavior after initial authentication completion. Device reputation analysis, network telemetry, interaction timing analysis, and behavioral consistency evaluation collectively reduced the effectiveness of MFA bypass campaigns.

The findings also revealed significant weaknesses associated with federation metadata management. Insecure metadata synchronization processes, delayed certificate updates, and weak trust validation procedures introduced opportunities for adversaries to manipulate authentication configurations or redirect trust relationships toward malicious endpoints. OAuth redirect URI vulnerabilities were similarly identified as high-risk attack vectors capable of enabling token interception and unauthorized authorization flow manipulation.

The study determined that centralized telemetry collection and integrated monitoring architectures substantially improved attack visibility across federated ecosystems. Organizations deploying Security Information and Event Management (SIEM) platforms integrated with authentication telemetry achieved more effective detection of anomalous authentication behavior, privilege escalation attempts, and cross-system attack propagation. Distributed logging architectures lacking centralized correlation capabilities demonstrated reduced forensic visibility and slower incident response effectiveness.

Repudiation analysis revealed that federated identity systems frequently suffer from fragmented audit trails distributed across multiple authentication entities. Identity providers, service providers, MFA vendors, and cloud services often maintain independent logging infrastructures with inconsistent timestamp synchronization and incomplete event correlation. These limitations complicate forensic investigations and reduce the reliability of attack attribution mechanisms.

The findings indicate that integrated logging frameworks improve organizational capacity to analyze authentication anomalies and reconstruct attack timelines. Systems implementing immutable audit logging, synchronized telemetry collection, and automated anomaly correlation demonstrated superior incident investigation capabilities compared to fragmented logging environments.

Denial of Service (DoS) analysis demonstrated that federated authentication infrastructures are highly sensitive to availability disruption because authentication failures propagate rapidly across dependent enterprise services. Authentication API flooding, federation

synchronization exhaustion, and MFA infrastructure overload attacks were identified as significant operational risks capable of disrupting enterprise continuity.

The research identified that layered resilience architectures significantly reduced the operational impact of availability attacks. Rate limiting, distributed identity infrastructure deployment, adaptive traffic filtering, failover authentication mechanisms, and automated workload balancing improved service continuity during simulated attack conditions. Organizations implementing layered defensive architectures achieved stronger operational resilience than environments relying on isolated perimeter defenses.

The comparative analysis of threat modeling methodologies revealed that hybrid frameworks combining STRIDE categorization, attack-centric modeling, and behavioral analysis produced more comprehensive security assessments than isolated analytical approaches. Traditional system-centric models effectively identified architectural vulnerabilities but frequently lacked visibility into adaptive adversarial behavior and operational attack progression. Conversely, purely attack-centric approaches emphasized adversary tactics but sometimes underrepresented infrastructure dependency relationships.

The integration of Cyber Kill Chain principles into the STRIDE framework improved the understanding of multi-stage attack progression within federated ecosystems. Attackers commonly progressed through reconnaissance, credential harvesting, MFA bypass, token exploitation, privilege escalation, and lateral movement phases. The combination of architectural threat categorization and operational attack sequencing therefore enhanced analytical depth and improved security prioritization.

The findings strongly support the integrated threat modeling perspective proposed by Eng (2017), which emphasizes the necessity of combining multiple analytical dimensions to evaluate interconnected security ecosystems effectively. The research demonstrated that federated identity infrastructures cannot be secured effectively through isolated authentication controls alone. Instead, security effectiveness depends on coordinated integration of contextual verification, adaptive monitoring, trust segmentation, certificate security, and behavioral intelligence.

The analysis additionally revealed that organizations adopting zero-trust security principles demonstrated stronger resilience against advanced authentication attacks. Continuous verification mechanisms, contextual trust scoring, least privilege access enforcement, and adaptive session monitoring collectively reduced the operational success of replay attacks, credential compromise campaigns, and lateral movement activities.

The findings further indicate that device fingerprinting technologies provide substantial operational value when integrated with adaptive authentication systems. However, the analysis also identified limitations associated with false positive generation, privacy concerns, and environmental variability. Highly dynamic user environments occasionally triggered legitimate authentication anomalies, thereby increasing operational complexity for security teams.

Another important finding relates to the growing importance of behavioral analytics within modern identity security architectures. Static authentication mechanisms increasingly fail to detect sophisticated adversaries operating with stolen credentials or compromised session artifacts. Continuous authentication approaches evaluating behavioral consistency, interaction patterns, and contextual trust indicators therefore represent critical future directions for federated identity protection.

The overall results confirm that federated SSO and MFA systems require comprehensive layered defense strategies integrating architectural security analysis, adaptive authentication, behavioral intelligence, centralized telemetry, and proactive threat modeling methodologies. Organizations implementing integrated threat detection and contextual trust evaluation mechanisms achieved significantly stronger resilience against both opportunistic and advanced persistent attack campaigns.

DECLARATION

The findings of this study provide strong evidence that federated SSO and MFA systems operate as deeply interconnected security ecosystems in which authentication integrity is dependent on multiple distributed trust relationships. The STRIDE-based analysis demonstrated that traditional assumptions about authentication security—particularly the belief that MFA alone is sufficient to prevent identity compromise—are increasingly inadequate in the context of modern cloud-

centric enterprise infrastructures. Instead, authentication security must be understood as an emergent property of interacting components including identity providers, service providers, token issuance mechanisms, device intelligence systems, and behavioral analytics frameworks.

A key theoretical implication of this research is the confirmation that STRIDE remains a valuable foundational model for structured threat categorization, but it requires augmentation with behavioral and attack-centric methodologies to fully capture adversarial dynamics in federated environments. As observed across the analysis, spoofing, tampering, and elevation of privilege threats frequently overlap in real-world attack scenarios such as token replay and golden SAML exploitation. This overlap suggests that discrete categorization alone is insufficient for modeling multi-stage attack campaigns. Eng (2017) emphasizes that integrated threat modeling approaches improve system-level visibility by combining multiple analytical perspectives, and the present study extends this argument by demonstrating its direct applicability to federated identity infrastructures.

From a practical security perspective, the results highlight a fundamental shift in attacker behavior. Modern adversaries increasingly target identity trust infrastructure rather than end-user credentials alone. The prevalence of golden SAML attacks illustrates this shift clearly, as attackers exploit compromised signing certificates to generate valid authentication assertions that bypass conventional security controls, including MFA enforcement. This undermines the traditional security assumption that authentication verification is sufficient to guarantee identity integrity. Instead, trust in federated systems becomes dependent on the security of underlying cryptographic and certificate management processes.

The analysis further reveals that token replay attacks and session hijacking represent persistent and operationally efficient attack vectors, particularly in OAuth-based environments that rely on bearer tokens. The ease with which intercepted tokens can be reused demonstrates a structural weakness in static authentication paradigms. While short-lived tokens and expiration policies reduce exposure windows, they do not eliminate risk in environments lacking contextual validation. The study therefore reinforces the importance of continuous authentication mechanisms and contextual trust evaluation systems.

Device fingerprinting emerged as a critical defensive enhancement; however, its effectiveness is not absolute. The findings indicate that while device intelligence significantly improves anomaly detection, it also introduces operational challenges including false positives, privacy concerns, and variability in user environments. For instance, legitimate users operating across multiple devices or dynamic network conditions may trigger risk-based authentication escalations. This highlights a trade-off between security sensitivity and usability, requiring organizations to calibrate adaptive authentication thresholds carefully.

The integration of Cyber Kill Chain analysis with STRIDE further improves the interpretability of federated attack progression. Attackers typically move through reconnaissance, credential harvesting, token exploitation, and privilege escalation phases before achieving full compromise. Mapping these stages onto STRIDE categories enhances the ability to identify where defensive controls are most effective. However, the study also shows that attackers often bypass linear progression models by exploiting trusted federation relationships, thereby compressing multiple attack phases into a single assertion compromise event.

Another important insight relates to the limitations of centralized versus distributed security architectures. While centralized SIEM systems significantly improve visibility and correlation of authentication events, they also introduce dependencies on data integration quality and synchronization consistency. Fragmented logging systems across identity providers and service providers reduce forensic accuracy, as noted in the results. Eng (2017) supports the necessity of integrated system visibility, and this study further demonstrates that without unified telemetry, federated threat detection becomes significantly less effective.

The research also highlights a growing alignment between federated identity security and zero-trust principles. Continuous verification, least privilege enforcement, and contextual access control mechanisms are essential to mitigating replay-based and assertion forgery attacks. However, the implementation of zero-trust architectures introduces additional computational overhead and operational complexity, particularly in large-scale enterprise environments with heterogeneous systems.

A notable contradiction identified in this study is that while MFA is widely regarded as a strong security mechanism, it does not meaningfully mitigate attacks targeting token integrity or federation trust infrastructure. This creates a false sense of security in organizations that over-rely on MFA without integrating complementary controls such as device intelligence, certificate protection, and behavioral analytics.

Overall, the discussion confirms that federated authentication security requires a multidimensional defense strategy that integrates structural modeling, behavioral analysis, and adaptive response mechanisms. The combination of STRIDE, attack-centric frameworks, and device-aware authentication provides a more realistic representation of modern threat environments than traditional isolated security models.

CONCLUSION

Federated SSO and MFA systems represent essential components of modern enterprise identity management infrastructures, yet they simultaneously introduce complex cybersecurity risks associated with distributed trust relationships, token exchange mechanisms, and adaptive authentication workflows. This research developed a STRIDE-based threat modeling framework for analyzing attack vectors affecting SP-initiated SAML and OAuth environments integrated with MFA and device fingerprinting controls.

The study demonstrated that token replay attacks, golden SAML exploitation, session hijacking, and MFA bypass techniques represent critical threats capable of compromising enterprise authentication ecosystems. Traditional static authentication controls were found insufficient against sophisticated adversaries employing multi-stage attack strategies and behavioral manipulation techniques.

By integrating STRIDE categorization with attack-centric analysis, behavioral monitoring, device fingerprinting, and layered defense architectures, the proposed framework improves visibility across federated authentication environments. The findings indicate that adaptive authentication mechanisms, contextual trust evaluation, centralized telemetry collection, and integrated threat intelligence significantly enhance cyber resilience.

This research contributes to existing cybersecurity literature by bridging gaps between architectural threat modeling, operational attack analysis, and adaptive identity security mechanisms. The study extends integrated threat modeling perspectives proposed by Eng (2017) and demonstrates the relevance of hybrid analytical methodologies within federated identity ecosystems.

Future research should focus on empirical validation through real-world security testing, AI-driven anomaly detection integration, privacy-preserving device fingerprinting mechanisms, and automated threat response orchestration. Additional investigation into zero-trust federation architectures and post-quantum authentication security may further enhance resilience against emerging cyber threats.

REFERENCES

1. Priyank Tailor, & Anjali Kale. (2025). Multimodal Sentiment Analysis of Earnings Calls and SEC Filings: A Deep Learning Approach to Financial Disclosures. Utilitas Mathematica, 122(1), 3163–3168. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2676
2. G. Krishnan and A. K. Bhat, "Empower Financial Workflows: Hyper Automation Framework Utilizing Generative Artificial Intelligence and Process Mining," 2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, 2025, pp. 2041-2047, doi: 10.1109/ICoICI65217.2025.11254280.
3. Abdul Salam Abdul Karim. (2023). Fault-Tolerant Dual-Core Lockstep Architecture for Automotive Zonal Controllers Using NXP S32G Processors. International Journal of Intelligent Systems and Applications in Engineering, 11(11s), 877–885. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/7749
4. Eng, D. (2017). Integrated Threat Modelling (Master's thesis, University of Oslo). Retrieved from http://hdl.handle.net/10852/55699
5. Carolina, I. R. &. I. M. D. N., USA, & Tiwari, S. K. (2025b). Automation Driven Digital Transformation Blueprint: Migrating legacy QA to AI augmented pipelines. Frontiers in Emerging Artificial Intelligence and Machine Learning, 2(12), 01–20.

https://doi.org/10.64917/feaiml/volume02issue12-01

6. Hutchins, Eric &Cloppert, Michael & Amin, Rohan. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Leading Issues in Information Warfare & Security Research. 1.

7. Hebbar, K. S., Sengupta, D., Armo, K. K., Sahu, P., Sahitya, P., & Rana, D. S. (2025). Integrating Sentiment Analysis with a Deterministically Optimized Extreme Learning Machine for Stock Market Prediction. 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG), 1–7. https://doi.org/10.1109/ictbig68706.2025.11323752

8. Kamati, Toivo Herman, Dharm Singh Jat, and Saurabh Chamotra. "Design and Development of System for Post-infection Attack Behavioral Analysis." Proceedings of Fifth International Congress on Information and Communication Technology: ICICT 2020, London, Volume 2. Singapore: Springer Singapore, 2020.

9. Kaur, Supinder, and Harpreet Kaur. "Client honeypot based malware program detection embedded into web pages." International Journal of Engineering Research and Applications 3.6 (2013): 849-854.

10. Krishnan, Sriram. (2017). A Hybrid Approach to Threat Modelling A Hybrid Approach to Threat Modelling. 10.13140/RG.2.2.33303.88486.

11. Liebl, Simon. (2023). Threat Modelling for Internet of Things Devices.

12. Lowe, H. J., Ferris, T. A., Hernandez, P. M., & Weber, S. C. (2009). STRIDE–An integrated standards-based translational research informatics platform. In AMIA annual symposium proceedings (Vol. 2009, p. 391). American Medical Informatics Association.

13. Martelleur, J., & Hamza, A. (2022). Security Tools in DevSecOps : A Systematic Literature Review (Dissertation). Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-118400

14. Nweke, L. O., &Wolthusen, S. (2020). A review of asset-centric threat modelling approaches.

15. Parsons, D. (2024, February 26). ICS Layered Threat Modeling | SANS Institute. https://www.sans.org/white-papers/38770/

16. Potteiger, B., Martins, G., &Koutsoukos, X. (2016, April). Software and attack centric integrated threat modeling for quantitative risk assessment. In Proceedings of the Symposium and Bootcamp on the Science of Security (pp. 99-108).

17. R. Laheri, "AI-Enhanced Biometric Systems for Insurance: Secure Authentication and Regulatory Compliance," 2025 2nd International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2025, pp. 1-6, doi: 10.1109/ICECONF65644.2025.11379513

18. Saini, V., Duan, Q., &Paruchuri, V. (2008). Threat modeling using attack trees. Journal of Computing Sciences in Colleges, 23(4), 124-131.

19. Sagar Kesarpu. (2025). Zero-Trust Architecture in Java Microservices. International Journal of Networks and Security, 5(01), 202-214. https://doi.org/10.55640/ijns-05-01-12

20. Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons.

21. Sidiroglou, S., &Keromytis, A. D. (2007). Composite Hybrid Techniques For Defending Against Targeted Attacks. In Malware Detection (pp. 213-229). Boston, MA: Springer US.

22. Subhash, P., Qayyum, M., Likhitha Varsha, C., Mehernadh, K., Sruthi, J., &Nithin, A. (2023, October). A Security Framework for the Detection of Targeted Attacks Using Honeypot. In International Conference on Computer & Communication Technologies (pp. 183-192). Singapore: Springer Nature Singapore.

23. Tatam, M., Shanmugam, B., Azam, S., &Kannoorpatti, K. (2021, January). A review of threat modelling approaches for APT-style attacks. Heliyon, 7(1), e05969. https://doi.org/10.1016/j.heliyon.2021.e05969

24. Viswanathan, G. (2021, January). A hybrid threat model for system-centric and attackcentric for effective security design in SDLC. In Web Intelligence (Vol. 19, No. 1-2, pp. 1-11). IOS Press.

25. Vishesh Goel. (2025). From Concierge to Cloud: Reimagining Hospitality Through SaaS-Driven Experiences. The American Journal of Engineering and Technology, 7(8), 38–52. https://doi.org/10.37547/tajet/Volume07Issue08-05

26. Valiveti, S. S. S. (2025). .NET Core microservices for Zero-Downtime AuthHub migrations. European Journal of Engineering and Technology Research, 10(5), 1–4. https://doi.org/10.24018/ejeng.2025.10.5.3288

27. 27. Vikram Singh, 2025, Policy Optimization for Anti-Money Laundering (AML) Compliance using AI Techniques: A Machine Learning Approach to Enhance Banking Regulatory Compliance, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 14, Issue 04 (April 2025)

28. 28. Wolf, A., Simopoulos, D., D'Avino, L., &Schwaiger, P. (2021). The PASTA threat model implementation in the IoT development life cycle. INFORMATIK 2020.

29. 29. Xiong, W. (2021). Enhancing IT Systems Cyber Resilience through Threat Modeling : Cyber Security Analysis of Enterprise Systems and Connected Vehicles (PhD dissertation, KTH Royal Institute of Technology). Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-300046

30. 30. Yeng, P. K., D., S., & Yang, B. (2020). Comparative Analysis of Threat Modeling Methods for Cloud Computing towards Healthcare Security Practice. International Journal of Advanced Computer Science and Applications, 11(11).