AMERICAN ACADEMIC PUBLISHER

INTERNATIONAL JOURNAL OF DATA SCIENCE AND MACHINE LEARNING (ISSN: 2692-5141)

Volume 04, Issue 02, 2024,
Published Date: - 02-10-2024
pages 55-73

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

Suresh Kumar Ganapathy
Independent Researcher, USA

Abstract

Federated authentication systems based on Single Sign-On (SSO) and Multi-Factor Authentication (MFA) have become fundamental components of modern enterprise identity and access management architectures. Organizations increasingly depend on Security Assertion Markup Language (SAML), OAuth 2.0, OpenID Connect (OIDC), and federated identity ecosystems to support cloud computing, distributed services, zero-trust architectures, and remote work infrastructures. Although these technologies improve usability, interoperability, and centralized authentication management, they also introduce complex attack surfaces involving identity providers, service providers, token exchanges, session management, trust relationships, and authentication workflows. Attack vectors such as token replay, credential theft, session hijacking, golden SAML attacks, MFA fatigue attacks, OAuth token abuse, and impersonation threats demonstrate the growing sophistication of adversaries targeting federated authentication environments. This study develops a comprehensive STRIDE-based threat modeling framework for analyzing attack vectors in federated SSO and MFA systems, particularly focusing on Service Provider (SP)-initiated SAML and OAuth deployments integrated with device fingerprinting and adaptive authentication controls.

The research synthesizes existing cybersecurity literature related to threat hunting, attack attribution, intrusion detection, cyber threat modeling, and defensive architectures to construct a structured analytical model for federated authentication ecosystems. The study evaluates threats across authentication phases including identity assertion generation, token transmission, session establishment, MFA verification, and trust federation management. The paper further examines how threat intelligence methodologies, MITRE ATT&CK mapping approaches, behavioral analysis, anomaly detection, and deception-based defensive techniques contribute to identifying and mitigating advanced authentication attacks. The proposed framework categorizes threats according to STRIDE dimensions—Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege—while analyzing their operational implications within enterprise infrastructures.

The findings indicate that federated identity systems are highly vulnerable to privilege escalation and identity manipulation when trust relationships are insufficiently validated or when token integrity protections are weak. Device fingerprinting, behavioral analytics, adaptive MFA enforcement, token-binding mechanisms, and continuous threat hunting significantly improve resilience against advanced adversarial techniques. However, limitations

remain regarding privacy concerns, false positives, federation scalability, and cross-domain trust dependencies. The study contributes a structured threat modeling methodology for securing federated identity ecosystems and provides practical recommendations for strengthening SSO and MFA deployments in enterprise and cloud environments.

Key words*: Federated Authentication, Single Sign-On, Multi-Factor Authentication, STRIDE Threat Modeling, SAML Security, OAuth Security, Golden SAML Attack, Token Replay, Device Fingerprinting, Identity and Access Management*

1. Introduction

The increasing adoption of cloud computing, distributed enterprise services, remote workforce models, and interconnected digital ecosystems has fundamentally transformed identity and access management architectures. Traditional standalone authentication mechanisms are no longer sufficient for organizations operating across multiple applications, cloud platforms, and heterogeneous environments. Consequently, federated identity systems based on Single Sign-On (SSO) and Multi-Factor Authentication (MFA) have emerged as critical technologies for centralized authentication management and secure user access control. Federated authentication frameworks such as Security Assertion Markup Language (SAML), OAuth 2.0, and OpenID Connect (OIDC) allow users to authenticate once and gain access to multiple interconnected services through trusted identity providers. These technologies significantly improve usability, operational efficiency, and user experience while reducing password fatigue and administrative overhead.

Despite their advantages, federated SSO and MFA systems introduce substantial cybersecurity challenges. The centralization of authentication processes creates high-value attack targets where successful compromise can provide adversaries with extensive access across multiple services and organizational domains. Threat actors increasingly exploit vulnerabilities associated with token issuance, assertion validation, trust federation relationships, session management, and MFA implementations. Attacks such as token replay, golden SAML manipulation, OAuth authorization abuse, session hijacking, MFA bypass, credential stuffing, and phishing-based impersonation demonstrate the complexity of securing federated identity infrastructures. Advanced persistent threat groups and cybercriminal organizations leverage these weaknesses to achieve unauthorized access, privilege escalation, persistence, and lateral movement across enterprise environments (Carbanak, 2017).

Threat modeling has therefore become an essential methodology for proactively identifying, analyzing, and mitigating risks within complex authentication architectures. STRIDE, originally developed as a systematic threat modeling framework, provides a structured mechanism for categorizing security threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The STRIDE methodology is particularly suitable for federated authentication systems because it enables comprehensive analysis of trust relationships, token integrity, communication channels, identity assertions, and session management mechanisms. Existing cyber threat modeling studies emphasize the importance of systematic attack surface analysis and representative security frameworks for modern enterprise environments (Bodeau et al., 2023). Furthermore, the evolution of cyber threat hunting techniques, attack attribution methodologies, and adversarial simulation models has reinforced the need for continuous monitoring and adaptive security strategies in identity ecosystems (Nour et al., 2023).

Modern federated authentication infrastructures operate within highly dynamic and distributed environments where multiple trust boundaries exist between identity providers (IdPs), service providers (SPs), users,

authentication brokers, cloud services, and external APIs. In SP-initiated SAML deployments, the authentication workflow often begins at the service provider before redirecting users to identity providers for verification. This process involves multiple token exchanges, session cookies, cryptographic assertions, and authentication states that can be manipulated if improperly secured. OAuth-based architectures introduce additional risks associated with authorization grants, token delegation, refresh tokens, and API access control. Adversaries frequently exploit misconfigurations, insecure token storage, weak certificate validation, and insufficient MFA enforcement to compromise authentication workflows.

Multi-Factor Authentication is widely recognized as a critical defense against credential compromise and unauthorized access. However, modern adversaries increasingly employ sophisticated bypass techniques including MFA fatigue attacks, push notification abuse, SIM swapping, session cookie theft, adversary-in-the-middle phishing frameworks, and token interception. Consequently, organizations are integrating adaptive authentication, behavioral analytics, device fingerprinting, and continuous verification mechanisms into federated authentication systems. Device fingerprinting enables authentication platforms to evaluate contextual characteristics such as browser attributes, device identifiers, geolocation patterns, operating systems, network behavior, and user interaction profiles to identify anomalous authentication attempts. These controls strengthen security posture by enabling risk-based authentication decisions and anomaly detection.

The significance of this research lies in addressing the lack of comprehensive threat modeling approaches specifically focused on federated SSO and MFA architectures integrating device fingerprinting and adaptive controls. Existing literature extensively discusses intrusion detection, cyber threat hunting, and attack attribution techniques, but comparatively fewer studies systematically apply STRIDE methodologies to modern federated identity ecosystems. This research bridges that gap by constructing a structured threat analysis framework tailored to SP-initiated SAML and OAuth deployments.

The primary objectives of this paper are fourfold. First, the study identifies critical attack vectors affecting federated SSO and MFA systems. Second, it applies the STRIDE threat modeling framework to classify and analyze authentication-related threats. Third, the study evaluates defensive mechanisms including device fingerprinting, adaptive MFA, threat hunting, and behavioral analytics. Finally, the research proposes a comprehensive threat mitigation framework for improving federated authentication security in enterprise environments.

The scope of this research encompasses federated authentication protocols, MFA systems, token management processes, identity federation architectures, attack attribution methodologies, and threat detection techniques. The study focuses specifically on enterprise-level deployments where trust relationships, authentication centralization, and distributed access management create complex attack surfaces. The findings contribute theoretical and practical insights into securing modern identity ecosystems while supporting cybersecurity professionals, enterprise architects, and researchers in designing resilient authentication infrastructures.

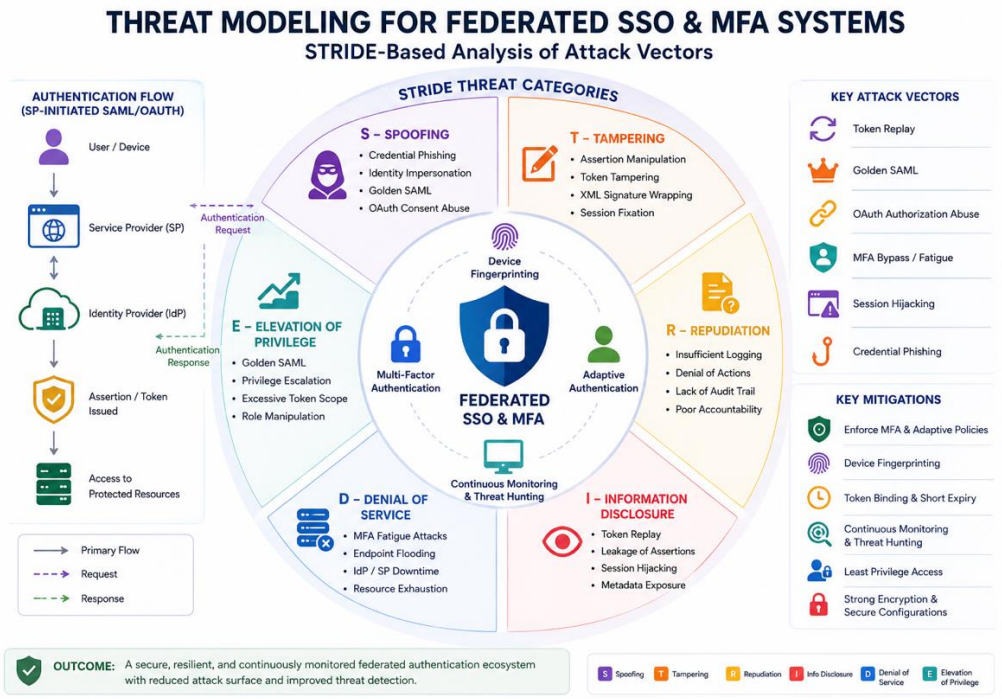

Figure 1. STRIDE-based threat modeling framework for Federated Single Sign-On (SSO) and Multi-Factor Authentication (MFA) systems. The figure illustrates the authentication flow between users, service providers, and identity providers while mapping security threats across the six STRIDE categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. It also highlights common attack vectors, including credential phishing, token replay, Golden SAML attacks, OAuth authorization abuse, session hijacking, and MFA fatigue attacks, together with corresponding mitigation controls such as adaptive authentication, device fingerprinting, least-privilege access, continuous monitoring, token protection, and strong encryption.

As illustrated in Figure 2, the STRIDE threat modeling framework provides a systematic approach for identifying and mitigating security risks within federated SSO and MFA environments. The model maps attack vectors to specific threat categories and supports the implementation of layered security controls to strengthen authentication resilience.

2. Literature Review

Cybersecurity research has increasingly emphasized the strategic importance of threat modeling, attack attribution, and proactive defense mechanisms in protecting modern enterprise infrastructures. The evolution of federated authentication architectures has expanded the complexity of attack surfaces, requiring integrated analytical approaches that combine identity security, threat hunting, intrusion detection, and behavioral analysis. Existing literature provides substantial insights into cyber threat modeling frameworks, attack detection methodologies, and defensive architectures relevant to federated SSO and MFA systems.

Bodeau, McCollum, and Fox highlighted the importance of structured cyber threat modeling frameworks capable of identifying vulnerabilities across complex digital infrastructures. Their work emphasized representative modeling approaches for analyzing attacker capabilities, system trust boundaries, and defensive control effectiveness. The study demonstrated that modern cyber threats increasingly exploit interconnected architectures where authentication systems serve as critical security dependencies. Their framework established foundational principles for systematic threat analysis applicable to federated identity ecosystems.

Threat attribution and targeted attack analysis have also become central themes in cybersecurity research. Kotenko and Khmyrov analyzed models and techniques used for attribution of cybersecurity violators involved in targeted attacks. Their work identified the increasing sophistication of adversaries leveraging identity manipulation and persistence strategies to evade detection. Similarly, Eichensehr discussed decentralized cyberattack attribution and the challenges associated with identifying malicious actors in distributed environments. These studies demonstrate the difficulty of detecting attacks within federated authentication infrastructures where multiple identity domains and trust relationships complicate attribution processes.

Threat hunting literature further reinforces the importance of proactive monitoring within authentication ecosystems. Nour, Pourzandi, and Debbabi provided a comprehensive survey of threat hunting in enterprise networks and argued that modern defensive architectures require continuous adversarial analysis rather than reactive security monitoring alone. Their study identified behavioral analytics, anomaly detection, and attack pattern recognition as critical mechanisms for detecting advanced threats. Mavroeidis and Jásang proposed data-driven threat hunting approaches using Sysmon telemetry to identify malicious system activities, demonstrating the value of behavioral monitoring in detecting abnormal authentication behavior.

Additional research has explored automated threat hunting and deception-based security strategies. Adedoyin and Teymourlouei examined methods for automating threat hunting and response, highlighting the importance of machine-driven anomaly detection in large-scale enterprise systems. Ajmal et al. investigated deception-driven cyber threat hunting within SCADA networks and demonstrated that adaptive defensive mechanisms significantly improve resilience against sophisticated attackers. Although these studies focus on broader cybersecurity environments, their methodologies are highly relevant to federated identity systems where advanced attackers attempt to establish persistence through credential compromise and session manipulation.

Intrusion detection research provides additional theoretical foundations relevant to federated authentication security. Ahmadian Ramaki, Rasoolzadegan, and Jafari conducted a systematic review of intrusion detection systems based on Hidden Markov Models (HMMs). Their findings demonstrated that probabilistic behavioral modeling improves the detection of anomalous activities across complex systems. Ourston et al. similarly explored applications of Hidden Markov Models for detecting multi-stage network attacks, emphasizing the effectiveness of sequential behavioral analysis in identifying coordinated attack campaigns. These methodologies can be applied to authentication ecosystems where abnormal login sequences, token usage patterns, and device anomalies indicate potential compromise.

Kar et al. analyzed SQL injection detection using Hidden Markov Models and demonstrated the broader applicability of behavioral modeling techniques to cybersecurity detection systems. Alghamdi further examined security applications of Hidden Markov Models, emphasizing their utility for pattern recognition, anomaly detection, and predictive threat analysis. Collectively, these studies support the integration of behavioral analytics into federated authentication environments to identify suspicious authentication activities and unauthorized access attempts.

The literature also emphasizes the strategic importance of MITRE ATT&CK frameworks and threat intelligence mapping methodologies. The MITRE ATT&CK framework provides structured adversarial techniques for analyzing attacker behavior across different attack stages. The CISA Best Practices for MITRE ATT&CK Mapping document highlights the operational value of standardized attack classification and adversarial analysis for enterprise defense. Stepanenko compared Russian FSTEC threat modeling methodologies with MITRE ATT&CK matrices and identified differences in threat categorization and attack representation. These comparative analyses demonstrate the importance of standardized frameworks for understanding attacker tactics targeting authentication systems.

Supply chain security research contributes additional insights regarding trust relationships and distributed infrastructures. Williams, Lueg, and Lemay examined supply chain security challenges and emphasized the growing complexity of interconnected enterprise ecosystems. Gould, Macharis, and Haasis analyzed the emergence of security concerns within supply chain management literature, while Urciuoli and Hintsa discussed gaps in adapting supply chain management strategies to security requirements. These studies are relevant to federated identity systems because trust federation architectures similarly depend on interconnected trust relationships between identity providers, service providers, and third-party platforms.

Emerging technologies such as distributed ledger systems have also been explored within cybersecurity contexts. Asante et al. investigated distributed ledger technologies for supply chain security management and demonstrated their potential for integrity verification and decentralized trust management. Although not directly focused on federated authentication, these approaches offer conceptual relevance for securing authentication assertions, token validation, and identity integrity processes.

Research concerning threat hunting methodologies and cyber deception further informs defensive strategies for federated systems. Javeed explored threat hunting using memory forensics and highlighted the importance of runtime artifact analysis for identifying malicious persistence mechanisms. Miazi et al. examined the design of cyber threat hunting games and emphasized simulation-based training for defensive preparedness. Threat hunting concepts are particularly applicable to federated authentication ecosystems where adversaries attempt to evade detection through stealthy session manipulation and token abuse.

The reviewed literature collectively demonstrates that modern cybersecurity research increasingly prioritizes proactive threat analysis, behavioral detection, and adaptive defensive architectures. However, significant research gaps remain regarding the application of STRIDE-based threat modeling specifically to federated SSO and MFA systems integrating device fingerprinting and adaptive authentication mechanisms. Existing studies often address isolated aspects of threat hunting, intrusion detection, or attack attribution without comprehensively analyzing the interconnected attack surfaces present within federated authentication ecosystems.

This study addresses these gaps by integrating STRIDE threat modeling with federated identity architectures, adaptive MFA controls, device fingerprinting techniques, and behavioral threat detection methodologies. The research contributes a comprehensive analytical framework capable of systematically evaluating attack vectors affecting modern SSO and MFA deployments.

3. Federated SSO and MFA Architecture

Federated authentication architectures are designed to centralize identity verification processes while enabling users to access multiple distributed services through trusted authentication mechanisms. Single Sign-On systems reduce credential management complexity by allowing users to authenticate once with a centralized Identity Provider (IdP) before accessing multiple Service Providers (SPs). Multi-Factor Authentication extends this architecture by requiring additional verification factors beyond passwords, including possession-based tokens, biometric identifiers, or contextual authentication signals.

In SP-initiated SAML deployments, authentication begins when a user attempts to access a protected resource hosted by a service provider. The service provider redirects the user to the identity provider for authentication. Upon successful verification, the IdP generates a signed SAML assertion containing authentication attributes and authorization information. The assertion is transmitted back to the SP, which validates the assertion and establishes

a user session. OAuth and OpenID Connect workflows follow similar principles but emphasize delegated authorization and token-based API access.

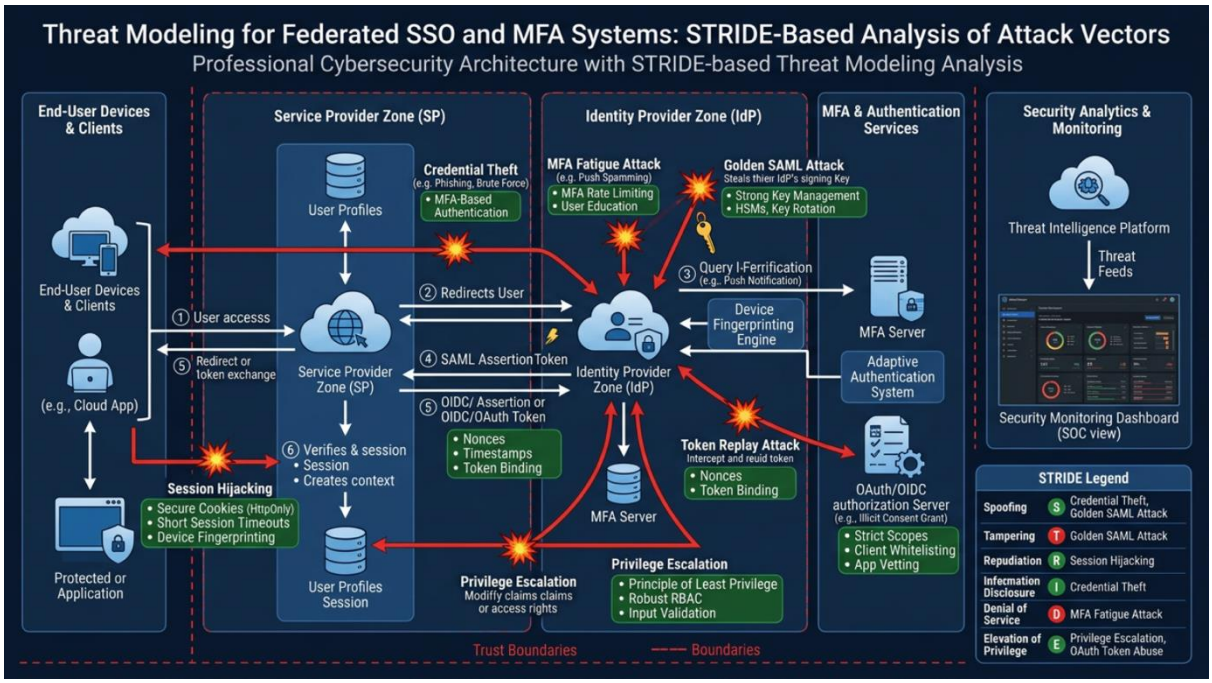

Figure 2. Security architecture of a federated Single Sign-On (SSO) and Multi-Factor Authentication (MFA) environment with integrated STRIDE-based threat mapping. The figure illustrates interactions between end-user devices, service providers (SPs), identity providers (IdPs), MFA services, OAuth/OIDC authorization servers, and security monitoring platforms. Major attack vectors—including credential theft, session hijacking, MFA fatigue attacks, Golden SAML attacks, token replay attacks, and privilege escalation—are mapped to trust boundaries and authentication flows. The architecture also highlights corresponding security controls such as adaptive authentication, device fingerprinting, token binding, role-based access control (RBAC), least-privilege enforcement, key management, client whitelisting, and continuous security monitoring.

As shown in Figure 2, federated SSO and MFA environments contain multiple trust boundaries across service providers, identity providers, authentication services, and authorization servers. These components create potential attack surfaces for credential theft, token abuse, privilege escalation, and session compromise. The architecture demonstrates how STRIDE-based threat modeling can be applied to identify security risks throughout the authentication lifecycle while simultaneously mapping preventive and detective controls to each attack vector.

Federated architectures introduce several trust boundaries involving users, browsers, identity providers, service providers, authentication brokers, MFA providers, and external APIs. Each trust boundary represents a potential attack surface where adversaries may intercept tokens, manipulate sessions, compromise trust relationships, or bypass authentication controls.

The integration of MFA into federated systems significantly improves authentication assurance but also increases architectural complexity. MFA workflows typically involve push notifications, one-time passwords, hardware tokens, or biometric verification. Adaptive MFA systems further incorporate contextual signals such as device reputation, geolocation, network behavior, and login history to dynamically assess authentication risk levels.

Device fingerprinting has emerged as a critical mechanism for contextual authentication analysis. Device fingerprinting collects behavioral and environmental characteristics including browser configurations, screen resolution, operating system details, IP addresses, installed plugins, hardware identifiers, and interaction patterns. These signals enable authentication systems to identify suspicious deviations from established user behavior profiles.

However, federated systems remain vulnerable to sophisticated attacks including token replay, session hijacking, golden SAML manipulation, OAuth consent abuse, credential phishing, and adversary-in-the-middle attacks. The centralized nature of identity providers amplifies risk because compromise of federation infrastructure may enable large-scale unauthorized access across interconnected services.

The complexity of modern federated architectures necessitates comprehensive threat modeling methodologies capable of evaluating interactions between authentication protocols, session management mechanisms, token validation processes, and adaptive security controls. STRIDE provides a structured framework for analyzing these multidimensional attack surfaces systematically.

4. STRIDE-Based Threat Modeling Framework

The STRIDE framework categorizes threats into six distinct categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Applying STRIDE to federated SSO and MFA architectures enables systematic identification of vulnerabilities across authentication workflows and trust boundaries.

4.1 Spoofing Threats

Spoofing attacks involve adversaries impersonating legitimate users, systems, or services. In federated authentication environments, spoofing commonly targets identity assertions, authentication sessions, or MFA workflows. Credential phishing remains one of the most prevalent spoofing techniques affecting SSO systems. Adversaries frequently deploy adversary-in-the-middle phishing frameworks capable of intercepting credentials, MFA tokens, and session cookies during authentication processes.

Golden SAML attacks represent advanced spoofing threats where attackers compromise identity provider signing certificates and generate forged SAML assertions. These forged assertions allow unauthorized access without requiring legitimate credentials or MFA verification. Because service providers trust signed assertions from identity providers, attackers can impersonate privileged users across federated environments.

OAuth-based systems are similarly vulnerable to token spoofing attacks involving malicious authorization requests, redirect URI manipulation, and consent phishing. Attackers may impersonate legitimate applications to obtain delegated access tokens and exploit API integrations.

Device fingerprinting provides partial mitigation against spoofing attacks by evaluating contextual authentication attributes. Authentication attempts originating from unfamiliar devices, abnormal geolocations, or suspicious browser configurations can trigger adaptive MFA challenges or access restrictions.

STRIDE Threat Modeling Matrix: Federated SSO & MFA Architecture

STRIDE Category	Attack Vector	Target Component	Risk Level	Security Impact	Mitigation Technique
Spoofing	• Identity impersonation	• Identity Provider (IdP)	High	• Unauthorized access • Session hijacking	• Certificate validation • Device fingerprinting • Strong client authentication
Tampering	• SAML assertion manipulation • Token modification	• Service Provider (SP) • OAuth Authorization Server	Critical	• Privilege escalation • Data integrity loss	• Digital signatures (XML/JWT signing) • Message integrity checks • Robust validation logic
Repudiation	• Log evasion • Deleting audit trails	• Session Manager • Logging Service	Medium	• Inability to investigate incidents • Compliance failure	• Immutable logging • Secure log transmission • Threat hunting • SIEM integration
Information Disclosure	• Token leakage • PII exposure in responses	• API Gateway • OAuth Authorization Server	High	• Data breach • Privacy violations	• Token binding • Transport Layer Security (TLS) • Minimal data disclosure principles
Denial of Service	• MFA flooding • Auth request exhaustion	• MFA Gateway • Identity Provider (IdP)	Medium	• System unavailability • Disruption of business operations	• Rate limiting • Anomaly detection • Adaptive MFA • Load balancing
Elevation of Privilege	• Golden SAML attack • Exploiting misconfigured scopes	• Identity Provider (IdP) • OAuth Authorization Server	Critical	• Full domain compromise • Administrative access gain	• Strong key management for signing certificates • Behavioral analytics • Regular security audits • Least privilege access controls

Figure 3. STRIDE Threat Modeling Matrix for Federated SSO and MFA Architecture

Figure 3. STRIDE threat modeling matrix for Federated Single Sign-On (SSO) and Multi-Factor Authentication (MFA) architecture. The matrix categorizes security threats according to the STRIDE framework and maps each threat to its associated attack vectors, target components, risk levels, security impacts, and mitigation techniques. The analysis identifies critical risks such as identity impersonation, SAML assertion manipulation, token leakage, MFA flooding, and Golden SAML attacks affecting identity providers, service providers, OAuth authorization servers, and MFA gateways. The matrix further demonstrates how security controls including certificate validation, digital signatures, secure logging, token binding, adaptive authentication, behavioral analytics, and least-privilege access can reduce attack exposure and improve the resilience of federated identity systems.

Figure 3 presents a comprehensive STRIDE threat modeling matrix for federated SSO and MFA environments. The matrix systematically maps threat categories to attack vectors, affected architectural components, risk severity levels, potential security impacts, and recommended mitigation controls. This structured approach enables security architects to prioritize high-risk vulnerabilities, evaluate attack paths, and implement appropriate defensive measures across identity providers, service providers, authorization servers, and authentication infrastructure.

4.2 Tampering Threats

Tampering threats involve unauthorized modification of authentication data, tokens, assertions, or session information. Federated systems heavily rely on XML assertions, JSON Web Tokens (JWTs), cookies, and session identifiers that can be manipulated if integrity protections are weak.

SAML assertion tampering occurs when attackers modify assertion contents including user identities, roles, or authorization attributes. XML signature wrapping attacks exploit weaknesses in XML validation logic by inserting malicious assertions alongside legitimate signatures. Improper token validation procedures significantly increase exposure to tampering attacks.

OAuth token tampering includes manipulation of refresh tokens, authorization codes, and JWT claims. Weak cryptographic protections or insecure token storage mechanisms enable attackers to alter token attributes or inject unauthorized privileges.

Session fixation attacks also represent tampering threats where attackers manipulate session identifiers before user authentication. Once authenticated, the victim unknowingly uses attacker-controlled sessions, enabling unauthorized access.

Cryptographic signing, token binding, secure session management, and integrity validation mechanisms are essential for mitigating tampering threats. Continuous token verification and strict schema validation further reduce exposure to manipulation attacks.

4.3 Repudiation Threats

Repudiation threats involve denial of performed actions or insufficient auditability within authentication systems. Federated environments often span multiple domains, making attribution and accountability challenging.

Attackers exploiting compromised sessions or stolen tokens may perform unauthorized actions while concealing their identities. Inadequate logging mechanisms, fragmented authentication records, and inconsistent federation monitoring complicate forensic investigations.

Threat hunting methodologies described by Nour et al. and Javeed emphasize the importance of centralized logging, behavioral analytics, and continuous monitoring for attribution analysis. Security Information and Event Management (SIEM) platforms integrated with authentication infrastructures improve accountability by correlating authentication events across multiple systems.

Non-repudiation mechanisms such as digitally signed assertions, immutable logging, timestamp validation, and behavioral tracking significantly improve investigative capabilities within federated systems.

4.4 Information Disclosure Threats

Information disclosure involves unauthorized exposure of sensitive authentication data including tokens, credentials, user attributes, session identifiers, and federation metadata.

Token replay attacks are particularly dangerous in federated systems because intercepted SAML assertions or OAuth tokens may provide immediate unauthorized access. Adversaries commonly exploit insecure transport mechanisms, browser vulnerabilities, and compromised endpoints to capture authentication artifacts.

Federation metadata leakage can reveal identity provider endpoints, certificate details, supported authentication methods, and trust relationships. Such information enables attackers to conduct targeted reconnaissance and exploit federation-specific vulnerabilities.

Device fingerprinting data also introduces privacy considerations because extensive behavioral profiling may expose sensitive user characteristics. Organizations must balance authentication security with privacy compliance and ethical data collection practices.

Encryption, secure transport protocols, token expiration policies, and data minimization strategies are essential for mitigating information disclosure risks.

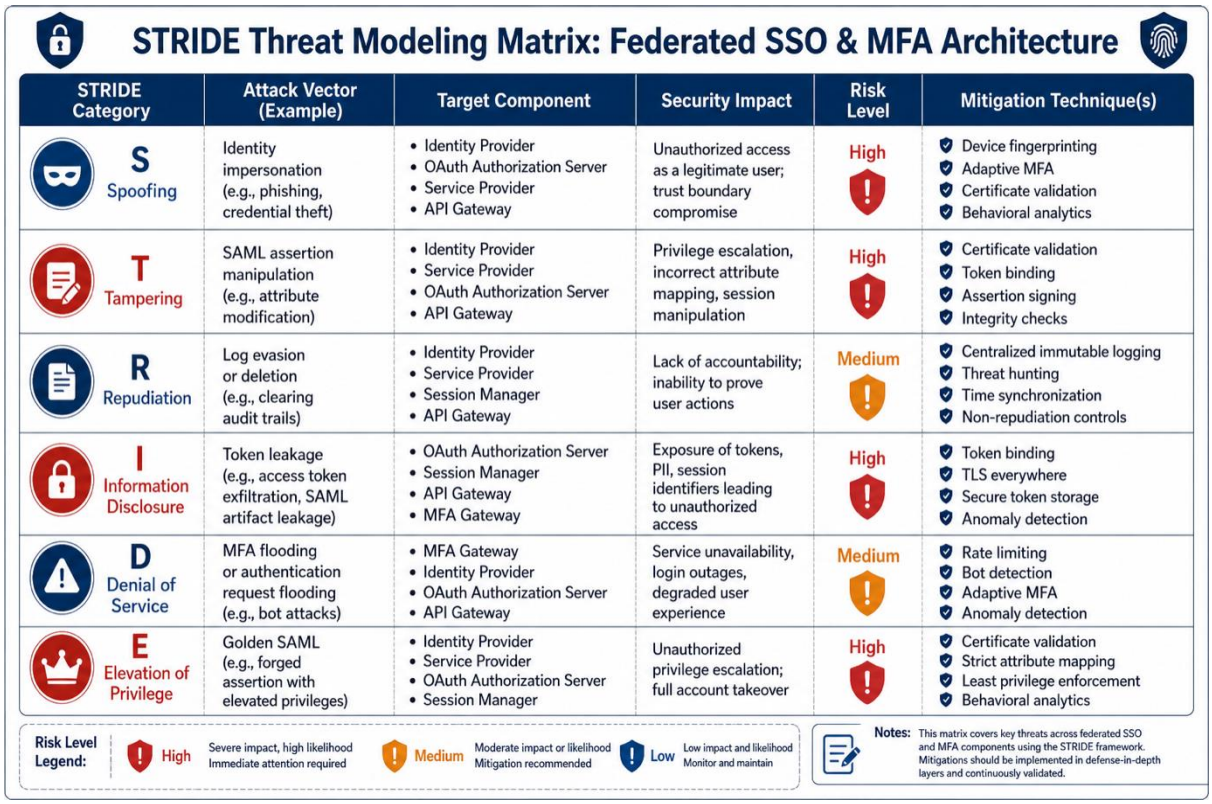

Figure 4. Enhanced STRIDE Threat Modeling Matrix for Federated SSO and MFA Architecture

Figure 4. Enhanced STRIDE threat modeling matrix for Federated Single Sign-On (SSO) and Multi-Factor Authentication (MFA) architecture. The matrix provides a detailed assessment of STRIDE threat categories by mapping representative attack vectors, affected system components, security impacts, risk levels, and corresponding mitigation techniques. The analysis covers threats including identity impersonation, SAML assertion manipulation, audit trail tampering, token leakage, authentication flooding, and Golden SAML privilege escalation attacks. Risk prioritization is supported through qualitative severity ratings, while defense mechanisms such as adaptive MFA, certificate validation, token binding, immutable logging, anomaly detection, behavioral analytics, and least-privilege enforcement are recommended to strengthen security across federated identity ecosystems.

Figure 4 presents an enhanced STRIDE threat modeling matrix that extends the architectural threat analysis by linking attack scenarios to specific target components, business impacts, risk severity levels, and mitigation controls. The matrix enables security teams to prioritize remediation efforts, evaluate defense-in-depth strategies, and implement appropriate controls for protecting federated SSO and MFA infrastructures against evolving identity-based attacks.

4.5 Denial of Service Threats

Denial of Service (DoS) attacks target authentication availability by overwhelming identity providers, MFA infrastructures, or federation services. Because federated authentication systems centralize identity verification, successful disruption may impact multiple enterprise applications simultaneously.

MFA fatigue attacks exploit push-notification-based authentication mechanisms by repeatedly triggering approval requests until users inadvertently approve malicious login attempts. Attackers increasingly automate these campaigns against enterprise users.

Resource exhaustion attacks targeting authentication endpoints, token validation services, or federation metadata exchanges can degrade authentication performance and disrupt business operations.

Adaptive rate limiting, distributed authentication infrastructures, CAPTCHA enforcement, and behavioral anomaly detection improve resilience against DoS attacks.

4.6 Elevation of Privilege Threats

Elevation of Privilege (EoP) attacks enable adversaries to obtain unauthorized administrative or privileged access. Golden SAML attacks represent one of the most severe EoP threats within federated systems because compromised signing certificates allow unrestricted assertion generation.

OAuth consent abuse also enables privilege escalation when malicious applications request excessive permissions or exploit overprivileged access scopes. Attackers may leverage compromised refresh tokens to maintain long-term persistence.

Insufficient role validation, weak authorization policies, and excessive trust delegation significantly increase EoP exposure. Federated environments often suffer from privilege inheritance issues where roles assigned by identity providers automatically propagate across interconnected services.

Zero-trust principles, least privilege enforcement, continuous access evaluation, and privilege segmentation are critical defensive mechanisms for limiting privilege escalation risks.

5. Attack Vectors in Federated SSO and MFA Systems

Federated authentication systems face increasingly sophisticated attack vectors targeting authentication workflows, trust relationships, and token management mechanisms.

5.1 Token Replay Attacks

Token replay attacks involve unauthorized reuse of captured authentication tokens or assertions. Adversaries may intercept SAML assertions through compromised endpoints, malicious proxies, browser vulnerabilities, or insecure network communications.

Replay attacks are particularly effective when tokens lack binding mechanisms or strict expiration policies. Attackers can reuse intercepted assertions across multiple services within federated ecosystems.

Mitigation strategies include token binding, short-lived assertions, cryptographic nonce validation, mutual TLS enforcement, and behavioral authentication analytics.

5.2 Golden SAML Attacks

Golden SAML attacks occur when adversaries compromise identity provider signing certificates and generate forged SAML assertions. These attacks bypass traditional authentication controls including MFA because service providers inherently trust signed assertions from identity providers.

Golden SAML attacks are highly dangerous within cloud environments because they enable unrestricted cross-service access. Adversaries often target Active Directory Federation Services (ADFS) infrastructures to obtain signing certificates.

Defensive strategies include hardware security modules (HSMs), certificate rotation policies, privileged access segmentation, behavioral anomaly detection, and continuous federation monitoring.

5.3 OAuth Authorization Abuse

OAuth ecosystems are vulnerable to malicious consent phishing, redirect URI manipulation, token leakage, and delegated authorization abuse. Attackers frequently exploit misconfigured applications to obtain excessive permissions.

Refresh tokens present significant risks because they provide long-term authorization persistence. Improper token revocation procedures further increase exposure.

Strict redirect validation, dynamic consent analysis, token scoping, and adaptive access controls are essential for securing OAuth deployments.

5.4 MFA Bypass Techniques

Modern attackers increasingly target MFA implementations through adversary-in-the-middle phishing, push fatigue attacks, SIM swapping, and session hijacking.

MFA fatigue attacks exploit human behavior by overwhelming users with repeated authentication prompts. Eventually, victims may approve malicious login requests unintentionally.

Device fingerprinting and behavioral analytics improve MFA resilience by identifying abnormal authentication contexts even when valid MFA approvals are obtained.

5.5 Session Hijacking

Session hijacking involves unauthorized acquisition of authenticated sessions through cookie theft, browser compromise, or token interception.

Adversaries frequently deploy malware capable of extracting session cookies from browsers. Once stolen, sessions may bypass MFA entirely because authentication has already been completed.

Secure cookie management, session rotation, endpoint protection, and continuous authentication validation reduce hijacking risks.

6. Device Fingerprinting and Adaptive Authentication

Device fingerprinting has emerged as a critical security mechanism for strengthening federated authentication systems against advanced adversarial techniques. Traditional authentication models rely heavily on static credentials and discrete MFA events, but sophisticated attackers increasingly bypass these controls through phishing, token theft, and session hijacking. Device fingerprinting introduces contextual intelligence into authentication workflows by evaluating environmental and behavioral characteristics associated with user devices and sessions.

Device fingerprinting systems collect multiple data attributes including browser versions, installed fonts, operating system configurations, screen resolutions, hardware identifiers, geolocation patterns, IP reputation, network behavior, and user interaction metrics. Machine learning and behavioral analytics techniques analyze these attributes to generate probabilistic trust scores reflecting authentication legitimacy.

Within SP-initiated SAML and OAuth workflows, device fingerprinting can operate during multiple authentication stages. During initial authentication requests, identity providers evaluate whether devices match previously observed behavioral baselines. Abnormal login patterns may trigger additional MFA challenges or access restrictions. Continuous authentication systems extend this process by monitoring post-authentication session behavior to identify deviations indicative of account compromise.

Adaptive authentication combines contextual intelligence with risk-based access control policies. Instead of applying uniform authentication requirements, adaptive systems dynamically adjust security measures according to calculated risk levels. High-risk authentication events involving unfamiliar devices, impossible travel patterns, TOR exit nodes, or abnormal user behavior may require additional verification or access denial.

The integration of behavioral analytics significantly enhances threat detection capabilities. Hidden Markov Model methodologies discussed by Ahmadian Ramaki et al. and Ourston et al. demonstrate the effectiveness of sequential behavioral analysis for identifying anomalous activities. Similar probabilistic models can analyze login sequences, token usage patterns, session transitions, and user interactions to identify suspicious authentication behaviors.

Despite their effectiveness, device fingerprinting systems introduce privacy and operational challenges. Excessive behavioral profiling may conflict with data protection regulations and user privacy expectations. Fingerprinting reliability may also decrease due to browser privacy protections, device changes, VPN usage, and legitimate behavioral variability.

False positives represent another critical limitation. Legitimate users traveling internationally or using new devices may trigger adaptive security mechanisms unnecessarily, negatively affecting usability and operational efficiency. Consequently, organizations must carefully balance authentication security with user experience and privacy considerations.

7. Threat Hunting and Detection Strategies

Threat hunting has evolved into a proactive cybersecurity discipline focused on identifying hidden adversarial activities within enterprise environments. Federated authentication systems particularly benefit from threat hunting methodologies because advanced attackers often maintain stealthy persistence through compromised identities, forged assertions, and stolen sessions.

Threat hunting methodologies discussed by Nour et al., Adedoyin and Teymourlouei, and Mavroeidis and Jásang emphasize behavioral monitoring, anomaly detection, and adversarial pattern analysis. Authentication-focused threat hunting involves monitoring login anomalies, token usage behaviors, session transitions, MFA approval patterns, and federation trust activities.

MITRE ATT&CK mapping provides structured adversarial analysis for authentication-related threats. Techniques such as Valid Accounts, Steal or Forge Authentication Certificates, Session Cookie Theft, Multi-Factor Authentication Interception, and Web Session Cookie manipulation are directly relevant to federated SSO systems.

Security Information and Event Management platforms enable centralized collection and correlation of authentication telemetry across identity providers, service providers, and cloud infrastructures. Correlation analysis improves detection of distributed attacks involving multiple authentication systems.

Memory forensics techniques described by Javeed are particularly valuable for detecting in-memory token theft and malicious session artifacts. Endpoint detection systems integrated with identity platforms improve visibility into authentication abuse scenarios.

Deception technologies further enhance detection capabilities by deploying honeytokens, decoy credentials, or fake federation endpoints designed to identify unauthorized access attempts. Attackers interacting with deceptive identity artifacts expose malicious intent and improve attribution capabilities.

Automated threat hunting systems increasingly leverage machine learning for authentication anomaly detection. Behavioral baselines enable rapid identification of unusual access patterns indicative of compromise. However, automated systems require continuous tuning to minimize false positives and maintain operational reliability.

8. Results and Findings

The STRIDE-based analysis conducted in this research identified significant vulnerabilities across federated SSO and MFA architectures, particularly within SP-initiated SAML and OAuth deployments. The findings demonstrate that authentication centralization substantially amplifies enterprise attack surfaces because compromise of identity providers or federation trust mechanisms can enable large-scale unauthorized access across interconnected services.

Spoofing threats emerged as one of the most severe categories affecting federated systems. Golden SAML attacks, credential phishing, adversary-in-the-middle frameworks, and OAuth consent abuse were identified as highly effective techniques capable of bypassing traditional authentication controls. The analysis revealed that compromised signing certificates represent critical security failures because service providers inherently trust assertions generated by identity providers. Device fingerprinting and adaptive MFA significantly improved detection capabilities against spoofing attacks by evaluating contextual authentication anomalies.

Tampering vulnerabilities primarily involved assertion manipulation, token modification, XML signature wrapping attacks, and insecure session management practices. Weak validation logic and improper token integrity controls substantially increased exposure to unauthorized privilege escalation. Federated systems lacking strict cryptographic enforcement demonstrated higher susceptibility to assertion forgery and replay attacks.

The analysis further demonstrated that information disclosure risks are strongly associated with insecure token storage, browser vulnerabilities, and session hijacking mechanisms. OAuth refresh tokens and long-lived session cookies represented particularly attractive attack targets because they enable persistent unauthorized access. Behavioral analytics and token-binding mechanisms significantly reduced replay attack effectiveness.

Threat hunting methodologies substantially improved visibility into advanced authentication attacks. SIEM integration, MITRE ATT&CK mapping, behavioral anomaly detection, and deception-based detection strategies enabled earlier identification of suspicious authentication activities. Machine learning-driven behavioral models were particularly effective in identifying abnormal session patterns and MFA bypass attempts.

Adaptive authentication and device fingerprinting mechanisms significantly improved resilience against credential-based attacks, but operational limitations were observed regarding false positives, privacy concerns, and device variability. Excessive contextual analysis occasionally affected legitimate user accessibility and authentication efficiency.

Overall, the findings confirm that federated SSO and MFA systems require continuous monitoring, behavioral analysis, strict cryptographic enforcement, and adaptive risk evaluation to maintain resilience against evolving adversarial techniques.

9. Discussion

The findings of this research highlight the growing strategic importance of threat modeling within federated identity ecosystems. As organizations increasingly adopt cloud-based infrastructures and distributed authentication architectures, identity systems have become central targets for advanced cyber adversaries. The STRIDE framework proved effective for systematically categorizing authentication threats and identifying critical vulnerabilities across federated workflows.

The analysis demonstrates that traditional perimeter-based security approaches are insufficient for protecting modern authentication ecosystems. Federated architectures fundamentally rely on trust relationships between identity providers, service providers, APIs, and external platforms. Consequently, compromise of centralized identity components can produce cascading security failures across enterprise infrastructures. Golden SAML attacks particularly illustrate this risk because attackers can exploit compromised signing certificates to bypass conventional authentication and authorization controls entirely.

The integration of device fingerprinting and adaptive MFA substantially strengthens authentication security by introducing contextual intelligence into access control decisions. Behavioral analytics, anomaly detection, and probabilistic authentication modeling significantly improve detection of compromised sessions and abnormal login behavior. These findings align with broader cybersecurity research emphasizing proactive threat hunting and behavioral defense strategies.

However, the research also identified important operational limitations. Device fingerprinting introduces significant privacy and regulatory concerns because extensive behavioral profiling may conflict with data protection requirements. Adaptive authentication systems also face challenges regarding usability and false-positive management. Excessively aggressive anomaly detection mechanisms may disrupt legitimate users and reduce operational efficiency.

The study further demonstrates that federated systems require continuous threat hunting capabilities rather than static security controls alone. Modern attackers increasingly employ stealth-oriented persistence strategies involving token theft, session manipulation, and delegated authorization abuse. SIEM correlation, deception technologies, behavioral monitoring, and MITRE ATT&CK mapping substantially improve detection capabilities against these threats.

Compared with existing literature, this research extends prior threat modeling studies by specifically focusing on SP-initiated SAML and OAuth environments integrated with adaptive authentication controls. Existing studies extensively discuss intrusion detection, attack attribution, and threat hunting, but comparatively fewer works systematically analyze federated authentication attack surfaces using STRIDE methodologies.

The research is limited by its conceptual and analytical scope because empirical deployment testing across large enterprise environments was beyond the study's operational constraints. Future research should evaluate real-world federated infrastructures using quantitative attack simulation models, adversarial emulation frameworks, and machine learning-based behavioral analysis systems.

10. Conclusion

Federated SSO and MFA systems have become foundational components of modern enterprise security architectures, enabling centralized identity management, distributed access control, and improved authentication usability. However, these systems also introduce highly complex attack surfaces involving trust federation, token management, session handling, delegated authorization, and adaptive authentication workflows.

This study developed a comprehensive STRIDE-based threat modeling framework for analyzing attack vectors affecting SP-initiated SAML and OAuth deployments integrated with MFA and device fingerprinting controls. The research identified critical threats including token replay attacks, golden SAML manipulation, OAuth authorization abuse, MFA bypass techniques, session hijacking, and privilege escalation attacks. The analysis demonstrated that centralized identity infrastructures significantly amplify enterprise risk exposure when trust relationships or token integrity protections are compromised.

The findings further revealed that behavioral analytics, adaptive authentication, device fingerprinting, threat hunting methodologies, and MITRE ATT&CK-based detection strategies substantially improve defensive resilience against advanced authentication attacks. However, operational limitations involving privacy concerns, false positives, federation complexity, and usability trade-offs remain significant challenges for organizations deploying adaptive security architectures.

This research contributes a structured analytical framework for evaluating federated authentication threats while integrating theoretical foundations from cyber threat modeling, intrusion detection, attack attribution, and behavioral security analysis. The study provides practical recommendations for strengthening federated identity ecosystems through continuous monitoring, strict cryptographic enforcement, contextual authentication analysis, least privilege enforcement, and proactive threat hunting strategies.

Future research should focus on empirical validation of adaptive authentication models, AI-driven threat detection systems, decentralized identity architectures, and quantitative assessment of behavioral anomaly detection effectiveness within large-scale enterprise environments.

References

1. A. Adedoyin and H. Teymourlouei, “Methods for Automating Threat Hunting and Response,” International Conference on Electrical, Computer, and Energy Technologies, ICECET 2021, 2021, doi: 10.1109/ICECET52533.2021.9698447.

2. A. Ahmadian Ramaki, A. Rasoolzadegan, and A. Javan Jafari, “A systematic review on intrusion detection based on the Hidden Markov Model,” Statistical Analysis and Data Mining: The ASA Data Science Journal, vol. 11, no. 3, pp. 111–134, Jun. 2018, doi: 10.1002/SAM.11377.

3. A.I. Belous, V.A. Solodukha, “Fundamentals of cybersecurity. Standards, concepts, methods and means of ensuring,” Eds Technosphere Moscow, 2021, p. 400–482.

4. “A SANS Survey,” 2016.

5. A. B. Ajmal, M. Alam, A. A. Khaliq, S. Khan, Z. Qadir, and M. A. P. Mahmud, “Last Line of Defense: Reliability through Inducing Cyber Threat Hunting with Deception in SCADA Networks,” IEEE Access, vol. 9, pp. 126789–126800, 2021, doi: 10.1109/ACCESS.2021.3111420.

6. Best Practices for MITRE ATT&CK Mapping. [Online]. Available: https://www.cisa.gov/uscertlsites/default/files/publications

7. B. Nour, M. Pourzandi, and M. Debbabi, "A Survey on Threat Hunting in Enterprise Networks," IEEE Communications Surveys and Tutorials, vol. 25, no. 4, pp. 2299–2324, 2023, doi: 10.1109/COMST.2023.3299519.

8. D. Javeed, "An Efficient Approach of Threat Hunting Using Memory Forensics," International Journal of Computer Networks and Communications Security, vol. 8, no. 5, pp. 37–45, May 2020, doi: 10.47277/IJCNCS/8(5)1.

9. D. J. Bodeau, C. D. McCollum, D. B. Fox. "Cyber Threat Modeling: Survey, Assessment, and Representative Framework." mitre.org. https://www.mitre.org/sites (accessed Feb. 1, 2023).

10. D. Kar, K. Agarwal, A. K. Sahoo, and S. Panigrahi, "Detection of SQL injection attacks using hidden markov model," Proceedings of 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016, pp. 1–6, Sep. 2016, doi: 10.1109/ICETECH.2016.7569180.

11. D. Ourston, S. Matzner, W. Stump, and B. Hopkins, "Applications of hidden Markov models to detecting multi-stage network attacks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences, HICSS 2003, pp. 10–19, 2003, doi: 10.1109/HICSS.2003.1174909.

12. D. V. Stepanenko, "Comparative review of information security threat modeling from the FSTEC methodology of Russia and MITRE ATT&CK matrices," Digital Technologies and Law: Collection of scientific papers of the I International Scientific and Practical Conference, vol. 6, pp. 337–346, Sept. 23,2022.

13. F. Aldauiji, O. Batarfi, and M. Bayousef, "Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art," IEEE Access, vol. 10, pp. 61695–61706, 2022, doi: 10.1109/ACCESS.2022.3181278.

14. Information on powers of FSTEC of Russia; list of regulatory legal acts determining these powers, (FSTEC of Russia). [Online]. Available: https://fstec.m/en/359-powers

15. I. V. Kotenko and S. S. Khmyrov, "Analysis of Models and Techniques Used for Attribution of Cyber Security Violators in the Implementation of Targeted Attacks." Voprosy kiberbezopasnosti, vol. 4, no. 50, pp 52–79, Sept. 2022, doi: 10.21681/2311-3456-2022-4-52-79.

16. J. E. Gould, C. Macharis, and H. D. Haasis, "Emergence of security in supply chain management literature," Journal of Transportation Security, vol. 3, no. 4, pp. 287–302, Oct. 2010, doi: 10.1007/S12198–010-0054-Z/METRICS.

17. J. S. Carbanak, "Threatens Critical Infrastructure: Cybercriminal APTs Merit Significant Investigation and Discussion," S. James, Washington, DC, USA : ICIT, 2017, 16 p.

18. K. E. Eichensehr, "Decentralized cyberattack attribution," American Journal of International Law, vol. 113, pp. 213–217, Oct. 2019.

19. L. Urciuoli and J. Hintsa, “Adapting supply chain management strategies to security - an analysis of existing gaps and recommendations for improvement,” International Journal of Logistics Research and Applications, vol. 20, no. 3, pp. 276–295, May 2017, doi: 10.1080/13675567.2016.1219703.

20. M. Asante, G. Epiphaniou, C. Maple, H. Al-Khateeb, M. Bottarelli, and K. Z. Ghafoor, “Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey,” IEEE Trans Eng Manag, vol. 70, no. 2, pp. 713–739, Feb. 2023. doi: 10.1109/TEM.2021.3053655.

21. M. N. S. Miazi, M. M. A. Pritom, M. Shehab, B. Chu, and J. Wei, “The design of cyber threat hunting games: A case study,” 2017 26th International Conference on Computer Communications and Networks, ICCCN 2017, Sep. 2017, doi: 10.1109/ICCCN.2017.8038527.

22. M. Stefano, “La strategia della Nato in ambito cyber ”, Avv. Stefano Mele, Presidente della Commissione Sicurezza Cibernetica del Comitato Atlantico Italiano, Italia, 3 Giugno 2019 [Online]. Available: https://europaatlantica.it

23. MITRE ATT&CK: Design and Philosophy, The MITRE Corporation. [Online]. Available: https://attack.mitre.org/docs

24. P. Samarati, “2013 International Conference on Security and Cryptography (SECRYPT) 29–31 July 2013, Reykjavík, Iceland; … part of ICETE 2013, 10th International Joint Conference on e-Business and Telecommunications ”.

25. R. Alghamdi, “Hidden Markov Models (HMMs) and Security Applications,” IJACSA) International Journal of Advanced Computer Science and Applications, vol. 7, no. 2, 2016, Accessed: Feb. 27, 2024. [Online]. Available: www.ijacsa.thesai.org.

26. Securing the Extended Internet of Things (XIoT), The Global State of Industrial Cybersecurity. [Online]. Available: https://claroty.com

27. Threat hunting, Welcome to Encyclopedia. [Online]. Available: https://encyclopedia.kaspersky.com/glossary/threat-hunting

28. V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, “A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures,” IEEE Internet Things J, vol. 8, no. 8, pp. 6222–6246, Apr. 2021, doi: 10.1109/JIOT.2020.3025775.

29. V. Mavroeidis and A. Jásang, “Data-driven threat hunting using sysmon,” ACM International Conference Proceeding Series, pp. 82–88, Mar. 2018, doi: 10.1145/3199478.3199490.

30. Z. Williams, J. E. Lueg, and S. A. Lemay, “Supply chain security: An overview and research agenda,” The International Journal of Logistics Management, vol. 19, no. 2, pp. 254–281, Aug. 2008, doi: 10.1108/09574090810895988/FULL/XML.