World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Secure enterprise authentication in the AI era: OAuth2, ADFS, and MFA in practice

Tamilmani Annamalai Raja *

College of Engineering, Guindy.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(02), 337–344

Publication history: Received on 18 April 2026; revised on 25 May 2026; accepted on 28 May 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.19.2.0286

Abstract

Enterprise authentication serves as a fundamental element of contemporary digital security because organizations depend on it to secure their cloud computing and distributed system and AI-based technology operations. Static credential-based authentication systems have become obsolete because they fail to protect against modern cyber threats, which include credential theft and identity spoofing and phishing attacks. The article evaluates three major enterprise authentication solutions through the lens of their development in AI-based threat detection systems, which include OAuth2 and Active Directory Federation Services (ADFS) and Multi-Factor Authentication (MFA). The paper defines security capabilities of each method through their operational implementations and architectural foundations while showing their security deficiencies, which include token flaws and federation flaws and usability flaws. Artificial intelligence (AI) creates disruptive authentication methods, which use behavioral biometrics and anomaly detection and adaptive access control to deliver authentication value. The comparative analysis shows how accessible these mechanisms operate in actual enterprise environments. The paper concludes by emphasizing the importance of implementing multiple authentication layers with secure implementation standards and AI security system integration. This review provides comprehensive knowledge about secure enterprise authentication systems, which protect organizations from AI-related security threats while supporting the development of effective identity management systems.

Keywords: Enterprise Authentication; OAuth2; ADFS; Multi-Factor Authentication; Artificial Intelligence

1. Introduction

The digital world needs current enterprise authentication systems to secure organizational networks from cyber threats. Security systems that base their protection on established boundaries now fail to safeguard operations which combine cloud computing and remote work and interconnected platforms. Modern enterprises utilize identity-based security systems to establish authentication systems as their primary defense mechanism against unauthorized entry attempts. The increased number of access points created by the new systems, which have emerged from this transition, has made identity systems the most targeted entity by cyber attackers [1]. The recent data indicates that credential theft and weak authentication methods account for most data breaches. Attackers can obtain unauthorized access to enterprise systems through various vulnerabilities which include password reuse, phishing attacks and token exploitation. Organizations are creating authentication systems which combine multiple authentication methods to build better security systems which include OAuth2 and ADFS and MFA as their identity verification tools [2]. The introduction of artificial intelligence (AI) has transformed the methods used in cybersecurity to defend against attacks and launch their own. AI supports authentication through its ability to implement risk-based access control systems that use behavioral biometrics and anomaly detection for authentication purposes. Adversaries use AI to create automated phishing systems, generate deepfake identities and use AI to bypass conventional authentication security systems. The dual-use nature of AI creates security challenges which affect both the protection of enterprise authentication systems and the evaluation of existing security systems [3].

* Corresponding author: Tamilmani Annamalai Raja.

The present study needs to identify common authentication technologies, their operational functions, their operational strengths, and their operational faults. OAuth2 enables distributed systems to use secure delegated access, while ADFS enables organizations to share identity information through identity federation, and MFA adds extra security to systems that depend on passwords. Organizations achieve success through these mechanisms when they establish correct security configurations together with security controls and systems that deal with future security threats [4]. The review paper examines authentication systems through their applicability to contemporary enterprise environments which AI technology creates. The research study analyzes the security weaknesses of OAuth2 and ADFS and MFA while establishing secure deployment methods to protect against security threats. The research study will help to establish a deeper understanding of secure enterprise authentication at the time of AI.

2. Evolution of Enterprise Authentication

The evolution of enterprise authentication systems traces a path that reflects the broader evolution of information systems from their inception in isolated on-premises systems to the current state of widespread distributed systems that use cloud-based architecture. The initial authentication systems created by users depended on password-based security, which depended on the usage of static credentials that were stored in centralized directories for verification purposes. The systems offered simple installation procedures but became vulnerable to multiple security threats which included brute force attacks, credential stuffing attacks, and phishing attacks. Organizations needed to move beyond single factor authentication when their systems expanded and their network connections increased, which required them to implement more advanced methods for identity management that offered both security and operational flexibility [5].

Directory services which introduced Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory were the foundation of the next major advancement in enterprise authentication technology. These systems enabled organizations to run all their applications through a single system which handled both identity management and authentication management for their entire organization. Organizations that required web-based authentication for their business ventures together with their need for cross-organizational collaboration encountered difficulties with directory-based authentication systems, which hindered their ability to deliver smooth and secure access. The Single Sign-On (SSO) solutions provide users with the capability to complete their authentication process one time, thus enabling them to access multiple systems without needing to provide their credentials at every login instance [6].

Federated identity management extended the original concept by enabling organizations to create trust relationships between their different domains and their partner domains. Security Assertion Markup Language (SAML) standards enabled identity providers to transmit authentication data securely to service providers, which formed the basis of this new method of user authentication and authorization. The method reduced the need for users to store multiple credentials across different systems while providing an easier user experience, but it introduced new difficulties related to establishing trust between parties and ensuring secure token management [7].

The rapid expansion of APIs, mobile applications, and cloud services created a growing requirement for authorization frameworks to become lighter and more adaptable. The above demand saw the development of OAuth2 and OpenID Connect, which shifted the focus towards identity authentication only to delegated authorization and secure access to resources. OAuth2 represents a new type of protocol that enables contemporary web applications to give third-party software access to user data while protecting user credentials from exposure. This system transformation changes authentication systems from a tightly integrated structure into a decentralized framework, which improves both system scalability and system capability to work with other systems [8].

The development of enterprise authentication systems has become more challenging because new security threats emerged to protect the organization against upcoming entry points of information. Authentication systems become vulnerable to attacks when users fail to properly set up their authentication systems, which leads to the creation of security loopholes and authentication token leaks. The current security framework of businesses has been developed to use multiple authentication mechanisms together with ongoing system checks and adaptive access security measures that react to shifting security threats. The historical evolution of technologies has enabled enterprises to use OAuth2, ADFS, and MFA for their security needs.

3. OAuth2 in Enterprise Security

The present-day enterprise systems which utilize cloud services, APIs and distributed systems have adopted OAuth2 as their standard authorization framework. OAuth2 enables applications to obtain protected resources through user-

based access control which allows users to provide access without giving their authentication information. The separation of authentication from authorization processing in OAuth2 has created a flexible framework which adapts to security needs in modern enterprise environments with multiple applications and services that require secure cross-boundary communications [9]. The primary components of OAuth2 core architecture consist of resource owner, client and authorization server and resource server. The authorization server provides access tokens to the client after the resource owner successfully authenticates. The use of this token-based structure enables organizations to expand their operations while reducing the frequency of authentication processes that require credential verification. Through its various grant types which include authorization code and implicit and resource owner password credentials and client credentials OAuth2 enables organizations to choose the appropriate security protection methods for diverse application requirements [10].

The authorization code grant in the enterprise environment is considered the most secure flow, especially in combination with Proof Key for Code Exchange (PKCE). It protects against interception attacks by decreasing their attack surface and it works effectively for web and mobile applications. Organizations can use OAuth2 to provide authentication services through their authorization framework while also connecting to other identity systems which include OpenID connect. The system has gained popularity in enterprise platforms which provide integration with identity providers and cloud-based solutions [11].

The security advantages of OAuth2 come with various challenges which create security difficulties for implementation. Attacks target access tokens because they can be intercepted during transmission or leaked from storage locations. Systems can be attacked through their weak settings which allow attackers to use poor redirect uri validation and improper scope definition and the likes. Authorization flows enable attackers to gain access through phishing attacks and unauthorized applications which use the authorization methods. The development of secure implementation methods which include short-lived tokens, secure storage systems and strict validation requirements becomes necessary because of existing vulnerabilities [12]. The enterprise authorization system uses OAuth2 as its main advancement which delivers secure and flexible access control that can grow with business needs. The system requires proper arrangement, coordination with complementary security frameworks like MFA and system of identity federation to work effectively. The AI-driven threat environment requires organizations to establish OAuth2 systems which can protect their authentication systems (Table 1, Figure1).

Table 1 Comparison of OAuth2, ADFS, and MFA

Feature	**OAuth2**	**ADFS**	**MFA**
Type	Authorization framework	Identity federation service	Authentication mechanism
Security Strength	Moderate	Moderate to high	High
Complexity	Moderate	High	Low to moderate
Common Risks	Token leakage, misconfiguration	Directory attacks, token forgery	Fatigue attacks, social engineering
Typical Use Case	API authorization, cloud access	Enterprise SSO and federation	Identity verification enhancement

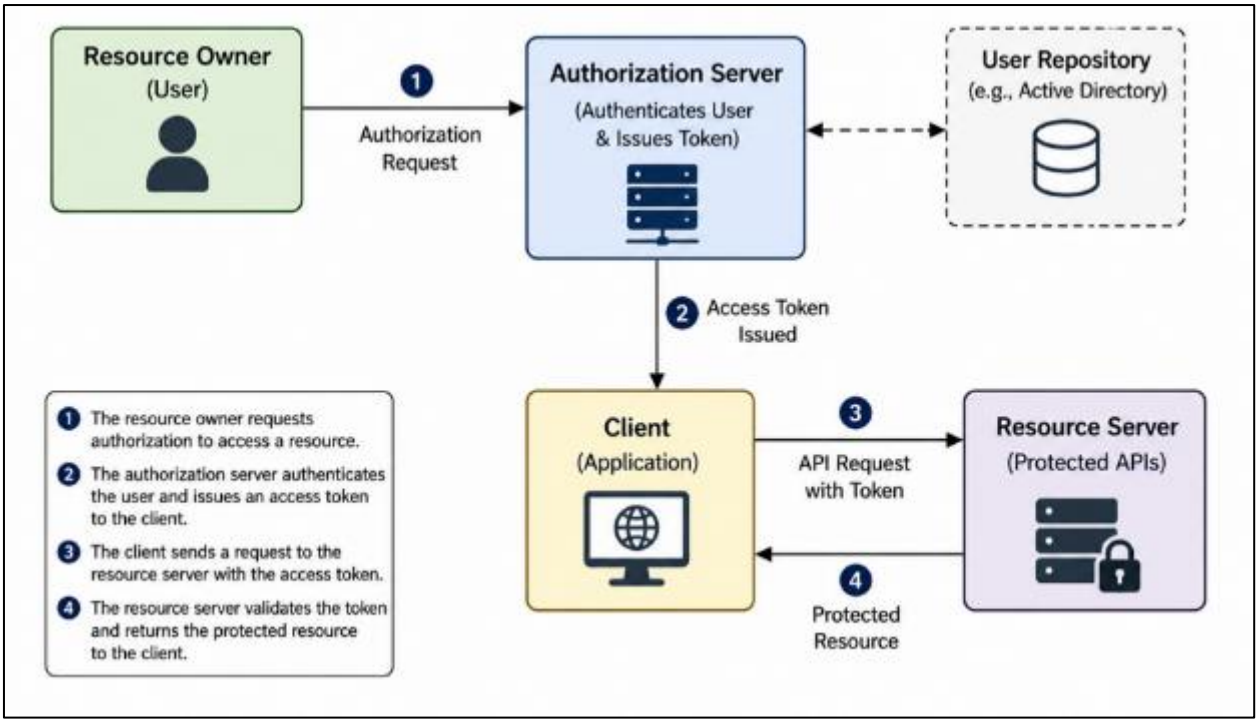

Figure 1 OAuth2 authorization framework architecture illustrates the interaction between the resource owner, client application, authorization server, and resource server.

4. Active Directory Federation Services (ADFS)

The enterprise authentication system uses Active Directory Federation Services (ADFS) to enable identity federation which enables users to access multiple applications and organizations through Single Sign-On (SSO). ADFS enables organizations to extend their internal identity systems for external service access while maintaining centralized control of their identity systems as more enterprises adopt hybrid cloud- hybrid systems that combine on-premises and cloud elements. Organizations use ADFS to permit single user authentication which enables users to access multiple authorized applications without the need for additional credential checks [13].

ADFS establishes trust relationships between identity providers and their relying parties who depend on their services. A user authentication process uses ADFS to verify Active Directory users before issuing a security token which contains user identity information. The application processes these claims to determine who should have access. ADFS supports multiple enterprise applications and legacy systems through its ability to work with various authentication protocols which include SAML and WS-Federation. The ability of ADFS to work with different systems has become a preferred choice for organizations that want to connect different security systems [14]. The main benefits ADFS provides to organizations stem from its ability to centralize identity management while establishing consistent security protection measures. Through one system administrators can create access control rules while they track user authentication activities and turn on multi-factor authentication. The system enables organizations to maintain regulatory compliance through its centralized design which enhances system visibility. ADFS enables organizations to connect their systems with cloud identity providers such as Microsoft Azure Active Directory which creates a unified identity solution for their hybrid identity systems that connect on-premises and cloud-based systems [15].

ADFS creates several security challenges along with operational difficulties that organizations need to address. The system suffers from both configuration and maintenance complexity which leads to misconfigurations that create security vulnerabilities. ADFS attackers use three main methods which include token forgery attacks and privilege elevation attacks that target Active Directory and trust relationship exploits. The attacker gains unauthorized entry to all federated systems when the service base becomes compromised. Security risks from outdated systems emerge because certain deployments rely on outdated security protocols which present security threats to their systems [16]. The authentication system contains ADFS as an essential yet sensitive component. The system functions through secure configuration which needs continuous scanning and as a security system which works with other security systems that include MFA and conditional access rules. ADFS needs proper management in enterprises which are shifting to cloud-native and AI-driven systems to achieve interoperability and usability together with security.

5. Multi-Factor Authentication (MFA)

The security of modern business systems depends on Multi-Factor Authentication (MFA) because it solves the security weaknesses which exist in single-factor authentication methods. The classical password-based authentication systems are highly vulnerable to various attacks including phishing attacks, credential stuffing and brute-force attacks. The application of MFA safeguards against dangers through its verification method which requires users to verify their identity by establishing two different authentication requirements from the three established identity authentication elements of the user password and the security token or mobile device and the user's biometric data. The system uses multiple security levels, which establishes user identity verification at higher levels, while it decreases potential security breaches [17].

Corporations use various methods to implement MFA through their security systems, which include one time passwords (OTPs), push-based authentication, a hardware token and biometric verification. The system creates authentication codes that expire after a certain period, which users need to enter by using a password together with push notifications. Biometric authentication systems (which use fingerprint or facial recognition) have become the standard authentication method for enterprise identity systems because they provide users with smoother authentication processes. Organizations can create authentication solutions based on their specific user needs and risk evaluation through this combination of multiple authentication methods, which offers them operational flexibility to choose from various techniques [18].

The technology of MFA has thorough documentation which shows its effectiveness to reduce security incidents throughout its history. Research shows that implementing an additional authentication method creates a strong defense against automated attacks, and it also minimizes the success rate of phishing attacks. Consequently, MFA is a frequently recommended control in security architectures and compliance measures as an important control measure in the protection of sensitive systems and information. The technology of OAuth2 and ADFS enables enterprise security to improve through its identity provider and authentication system combination, which adds a second verification layer to current access control systems [19].

MFA establishes its own security limits because new threats continue to emerge against its existing advantages. Through the repeated authentication prompts, attackers use MFA fatigue attacks to trick users into approving their malicious attempts to access the system. OTP systems that use SMS are vulnerable to SIM-swapping attacks which allow hackers to access SMS messages, while advanced phishing methods can capture authentication codes during their transmission. Unresolved usability problems will lead users to adopt unsafe workarounds because they experience login difficulties and they resist using the system. The existing limitations demonstrate the need to adopt advanced MFA systems, which should include hardware-based tokens and phishing-resistant authentication systems to create secure authentication environments [20].

MFA continues to serve as a vital component of enterprise authentication methods, which operate in the AI era. Organizations can use MFA together with adaptive authentication and behavioral analytics, which creates security controls that function based on contextual information of each specific situation. Yet organizations should continue their efforts to maintain security protection while making their systems easier to use by updating their MFA systems to adapt to new security threats and technological developments.

6. AI in Authentication Systems

The implementation of adaptive context-aware behavior-based security features has started to change enterprise authentication systems through their introduction of AI technology. Current authentication systems depend on fixed credentials together with established rules which show insufficient capabilities for detecting advanced and upcoming security threats. AI authentication systems provide users with better security because they continuously monitor user behavior patterns together with device characteristics and location information to maintain security at its highest level. Risk-based authentication models become operational through this system, which enables access management to modify access rights based on detected possibility of suspicious behavior [21]. AI has developed behavioral biometrics into a key technology which enables secure authentication processes. Behavioral biometrics enables authentication through the analysis of user behavior patterns, which includes their typing speed and mouse movements and touchscreen interface usage. The security system provides continuous unobtrusive authentication because its patterns are extremely difficult for attackers to reproduce. The process of behavioral signals through machine learning algorithms enables systems to detect real-time system anomalies, which serve as indicators of potential credential breaches or unauthorized access attempts [22].

AI technologies enable authentication systems to detect fraud while identifying unusual behavior patterns. AI models utilize extensive data sets together with advanced analytical techniques to identify specific user behavior patterns, which will help detect hidden user behavior anomalies that traditional systems could not find through rule enforcement. The enterprise authentication system becomes more effective through this function because it enables daily handling of authentication requests, which occur in large numbers. AI systems can identify suspicious behavior, which results in the activation of additional authentication procedures that include multi-factor authentication or complete access restriction to decrease the risk of unauthorized entry [23].

AI integration into authentication systems creates multiple security risks. The adversaries who use AI technology to enhance their attack skills have developed convincing phishing campaigns and deepfakes to impersonate people. Attackers can use deep learning to create fake voices, images, or videos that can circumvent biometric authentication systems. Authentication systems face security challenges because automated attack tools enable attackers to exploit authentication protocols, which creates a situation that requires more effort to defend against than traditional defense systems [24].

The major problem of authentication depends on the stability and transparency of AI models, which show two key issues. The user experience and security of applications get affected by model bias problems, false positive results, and the system's inability to provide explanations. Inaccurate security threat evaluation results in legitimate users getting denied access, while the system subjects them to unnecessary security procedures. The use of adversarial machine learning, a specific type of machine learning, enables users to manipulate AI models by inserting custom-made input data that the AI system cannot detect. Strong model validation requires continuous monitoring together with security system integration, which needs to protect against both internal and external security threats [25]. Authentication systems of enterprises now use AI technologies to develop intelligent platforms that include both established authentication methods and modern machine learning-based systems. Organizations must handle security risks through innovation while implementing security measures. The organizations need to follow a complete organizational strategy by combining AI capabilities with governance frameworks and safety measures and continuous security risk evaluation to achieve their goals of establishing resilient authentication systems (Figure 2).

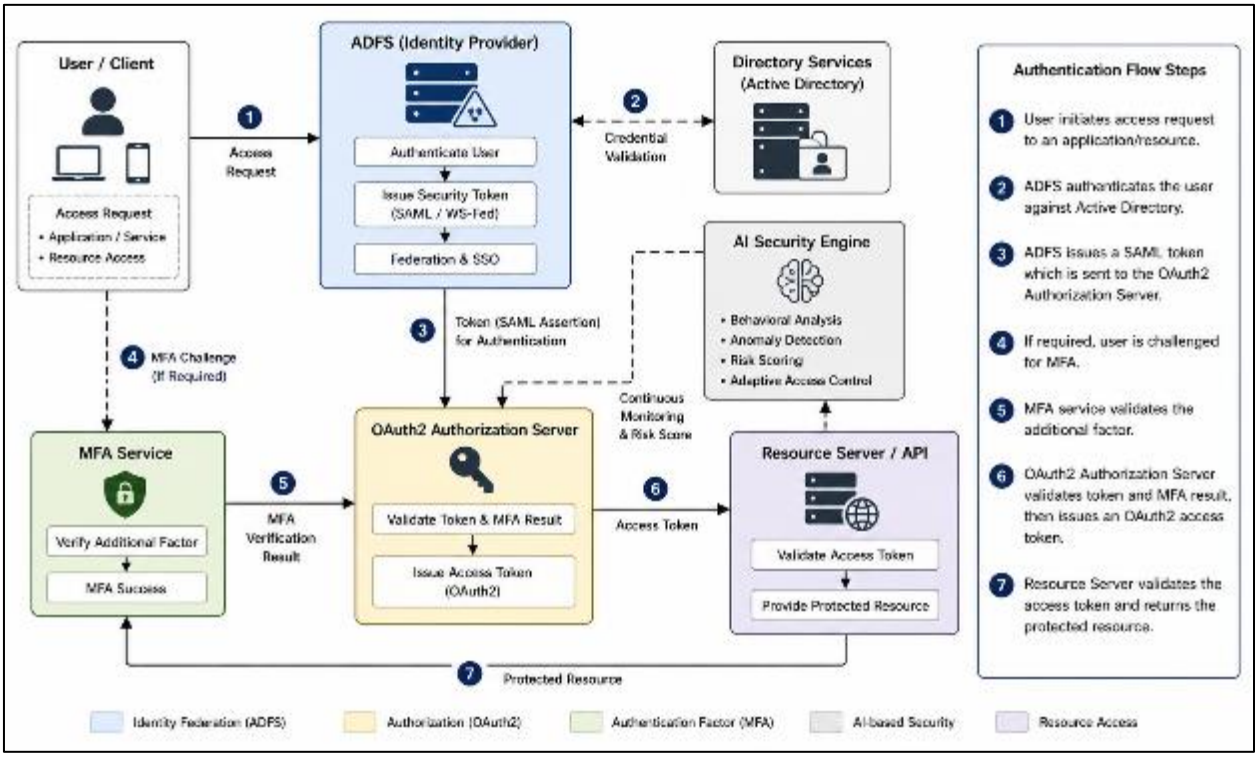

Figure 2 Integrated enterprise authentication framework

7. Future Directions

The modern enterprise authentication system now employs advanced identity systems which provide better security and user-friendly authentication methods that function without standard authentication methods. Password-free

authentication methods will become common because biometric systems, hardware security keys, device trust models will enhance security and user experience. The new identity management systems which use blockchain technology for decentralized user control now allow users to handle their digital identities without needing centralized identity management systems. Artificial intelligence will remain essential for authentication because it enables organizations to establish verification systems that continuously adapt to changing situations. Future systems will use behavioral analytics combined with real-time risk assessment and zero trust architectures to create access controls that will adjust dynamically based on operational requirements. The development of new technologies requires organizations to establish privacy protection systems together with AI transparency systems and defense mechanisms against adversarial threats. The development of authentication systems will progress through their ability to balance three main elements which include security requirements, usability needs and user trust requirements across increasingly advanced digital environments.

8. Conclusion

Enterprise authentication systems have changed their operations because digital infrastructure systems became more complex and AI-based cyber threats emerged. The current security requirements cannot be met through any single authentication method, according to this review. ADFS enables users to build a centralized identity federation that works with OAuth2 to provide scalable identity federation. MFA functions as a secure identity verification method through its implementation of multiple security layers. Both methods contain specific vulnerabilities that can be exploited when their implementation and control procedures are not executed properly. The implementation of artificial intelligence creates both new possibilities and new dangers because it expands detection capabilities while enabling advanced attack methods. Organizations must implement an authentication system that uses multiple technologies while they monitor their risk through continuous system monitoring. Organizations must achieve a balance between usability requirements, scalability needs, and security requirements to protect vital systems and sensitive data in the AI digital era.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Verizon. (2023). *Data breach investigations report*. Verizon Enterprise, 16(1), 1-120.

[2] Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines. *NIST Special Publication*, 800(63), 1-128.

[3] Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, 54(5), 3849-3886.

[4] Hardt, D. (2012). The OAuth 2.0 authorization framework. *IETF RFC*, 6749(1), 1-76.

[5] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security*, 89-98.

[6] Microsoft. (2021). Active Directory domain services overview. *Microsoft Documentation*, 1(1), 1-25.

[7] Cantor, S., Kemp, J., Philpott, R., & Maler, E. (2005). Assertions and protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. *OASIS Standard*, 2(0), 1-116.

[8] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014). OpenID Connect core 1.0 incorporating errata set 1. *OpenID Foundation*, 1(1), 1-76.

[9] Lodderstedt, T., McGloin, M., & Hunt, P. (2013). OAuth 2.0 threat model and security considerations. *IETF RFC*, 6819(1), 1-71.

[10] Fett, D., Küsters, R., & Schmitz, G. (2017). A comprehensive formal security analysis of OAuth 2.0. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 1204-1215.

[11] Jones, M. B., Bradley, J., & Sakimura, N. (2015). JSON Web Token (JWT). *IETF RFC*, 7519(1), 1-30.

[12] Parecki, A. (2019). OAuth 2.0 simplified: A practical guide to building secure applications. *Journal of Web Engineering*, 18(4), 301-320.

[13] Microsoft. (2022). Active Directory Federation Services overview. *Microsoft Learn Documentation*, 1(1), 1-30.

[14] Hughes, J., Maler, E., & Mishra, P. (2005). Security Assertion Markup Language (SAML) V2.0 technical overview. *OASIS Standard*, 2(0), 1-38.

[15] Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *NIST Special Publication*, 800(144), 1–80.

[16] Mandiant. (2021). ADFS security risks and attack techniques in enterprise environments. *Mandiant Threat Intelligence Report*, 1(1), 1–25.

[17] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, 2(1), 1–27.

[18] Das, A., Borisov, N., & Caesar, M. (2016). Do you hear what I hear? Fingerprinting smart devices through embedded acoustic components. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 441–452.

[19] Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *IEEE Symposium on Security and Privacy*, 553–567.

[20] NIST. (2017). Digital identity guidelines: Authentication and lifecycle management. *NIST Special Publication*, 800(63B), 1–74.

[21] Shrestha, A., Mahmood, A., Saxena, N., & Tamrakar, S. (2020). A survey of multi-modal biometric authentication using machine learning techniques. *IEEE Access*, 8(1), 167571–167593.

[22] Meng, W., Li, W., Su, Y., Zhou, J., & Lu, R. (2020). Enhancing user authentication through keystroke dynamics and machine learning. *Journal of Network and Computer Applications*, 147(1), 102437–102450.

[23] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58.

[24] Nguyen, T. T., Nguyen, Q. V. H., Nguyen, D. T., Nguyen, D. T., Nahavandi, S., & Nguyen, T. N. (2019). Deep learning for deepfakes creation and detection: A survey. *Computer Vision and Image Understanding*, 1(1), 102–115.

[25] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84(1), 317–331.