JTE HCM-UTE
ISSN: 2615-9740

JOURNAL OF TECHNICAL EDUCATION SCIENCE
Ho Chi Minh City University of Technology and Engineering
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn

Adaptive Multi-Factor Authentication With Federated and Temporal Learning: A Survey

Trung Kien Pham, Tan Kien Le*, Vinh Thinh Le
Ho Chi Minh City University of Technology and Engineering, Vietnam

*Corresponding author. *Email: 2591309@student.hcmute.edu.vn*

ARTICLE INFO

Received: 13/01/2026
Revised: 03/02/2026
Accepted: 09/04/2026
Online First: 08/05/2026
Published:

KEYWORDS

Adaptive Multi-Factor Authentication (Adaptive MFA);
Federated Learning;
Temporal Graph Learning;
Authentication Security;
Risk-Based Authentication.

ABSTRACT

Multi-Factor Authentication (MFA) has become a fundamental security mechanism for protecting modern information systems against credential-based attacks. While empirical studies have demonstrated that MFA significantly reduces account compromise, most deployed solutions rely on static authentication policies that introduce unnecessary user friction and remain vulnerable to advanced attacks such as phishing proxies and MFA fatigue. To address these limitations, adaptive and risk-based authentication mechanisms have been proposed, but they commonly depend on centralized data collection and centralized machine learning, raising serious concerns regarding privacy, scalability, and regulatory compliance. This survey provides a comprehensive review of adaptive MFA systems with a particular focus on Federated Learning (FL) as a privacy-preserving alternative to centralized authentication models. This survey presents a structured taxonomy of authentication frameworks based on authentication strategy, learning paradigm, and data modality, and systematically analyze existing FL-based risk-based authentication approaches. Furthermore, the survey highlights the importance of modeling authentication behavior as temporal and relational data and discuss how federated temporal graph learning can enable expressive yet privacy-aware authentication. Finally, this paper reviews commonly used datasets and evaluation practices and identify key open challenges and future research directions. This survey aims to serve as a reference and roadmap for researchers and practitioners designing next-generation adaptive and privacy-preserving authentication systems.

Doi: https://doi.org/10.54644/jte.2026.2075

1. Introduction

1.1. Motivation

User authentication is a fundamental security mechanism in modern information systems. Password-based authentication has long been the primary method, but it is increasingly ineffective against large-scale threats such as phishing, credential stuffing, and password reuse [1]. Multi-Factor Authentication (MFA) has therefore become widely adopted to strengthen security by requiring additional factors such as one-time passwords, push notifications, or biometrics. MFA also plays a key role in Zero Trust architectures through continuous verification [2], [3].

However, most MFA deployments still use static policies that apply the same authentication requirements to every login attempt. This approach creates two major problems: it increases user friction for legitimate users even in low-risk situations and fails to adequately defend against advanced attacks such as adversary-in-the-middle phishing, session hijacking, and MFA fatigue.

Adaptive and Risk-Based Authentication (RBA) has emerged as a promising solution. These systems dynamically adjust authentication strength based on estimated risk derived from contextual signals (device, location, time), behavioral patterns, and temporal features. Low-risk logins can proceed with minimal friction, while high-risk attempts trigger stronger verification. Despite its advantages, most

existing adaptive MFA systems rely on centralized data collection and machine learning, raising serious concerns about user privacy, regulatory compliance, scalability, and data governance.

1.2. Federated Learning for Authentication

Federated Learning (FL) offers a privacy-preserving alternative to centralized models. In FL, models are trained collaboratively across multiple clients (devices or organizational domains) while keeping raw data local. Only model updates are shared and aggregated at a central server [4]. This paradigm is well-suited for authentication because the data is highly sensitive and naturally distributed.

FL enables cross-domain collaboration and personalization without exposing raw authentication logs. However, authentication data is heterogeneous, temporally evolving, and subject to non-IID distributions, while FL itself introduces challenges such as model poisoning and inference attacks.

This survey provides a structured overview of research at the intersection of Multi-Factor Authentication, Adaptive/Risk-Based Authentication, and Federated Learning. Unlike previous surveys that focus mainly on MFA mechanisms or protocols, this work emphasizes learning-based and privacy-preserving approaches in distributed settings. It presents a taxonomy of authentication frameworks, reviews existing FL-based systems, highlights the value of temporal and relational modeling, and discusses open challenges and future directions.

The remainder of this paper is organized as follows: Section 2 reviews background concepts, Section 3 discusses the threat landscape, Section 4 presents a taxonomy, Section 5 surveys FL-based authentication systems, Section 6 examines temporal and relational modeling with a federated perspective, Section 7 covers datasets and evaluation practices, and Section 8 concludes with future research directions.

2. Background and Preliminaries

This section introduces the core concepts of Multi-Factor Authentication, adaptive/risk-based authentication, and Federated Learning that form the foundation for the rest of this survey.

2.1. Fundamentals of Multi-Factor Authentication

Authentication verifies the identity of a user or device accessing a system. Traditional single-factor authentication (mainly passwords) is increasingly insufficient due to phishing, credential stuffing, and password reuse.

Multi-Factor Authentication (MFA) improves security by combining two or more independent factors from different categories [5], [6]:

- Knowledge factors: something the user knows (e.g., passwords, PINs).
- Possession factors: something the user has (e.g., hardware tokens, smartphones, OTP generators).
- Inherence factors: something the user is (e.g., fingerprints, face recognition).
- Behavioral factors: something the user does (e.g., typing rhythm, mouse movements).

Although MFA significantly reduces unauthorized access, most deployments still use static policies that apply the same factors to every login attempt. This creates unnecessary user friction in low-risk situations and limited protection against advanced attacks.

Figure 1 illustrates the main categories of authentication factors used in MFA, including knowledge, possession, inherence, and behavioral factors.

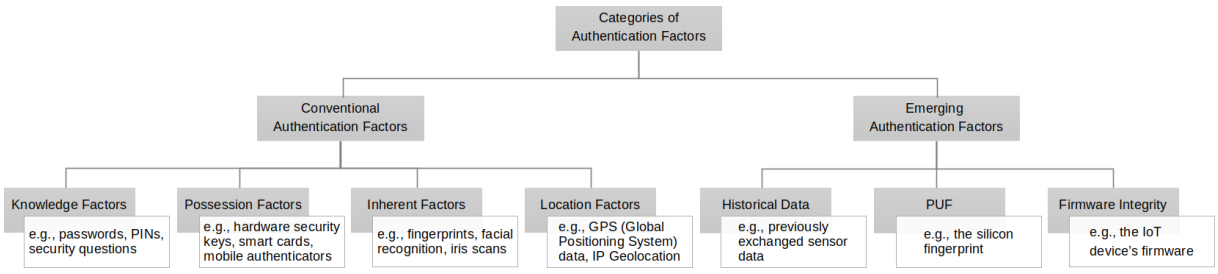

Figure 1. *Taxonomy of authentication factors* [7].

2.2. Adaptive and Risk-Based Authentication

Adaptive Authentication, also known as Risk-Based Authentication (RBA), dynamically adjusts the authentication requirements based on the estimated risk of each login attempt [8]. Risk is calculated from contextual signals (device, location, IP, time), behavioral patterns, and temporal features.

Low-risk attempts may allow password-only access, while high-risk attempts trigger additional factors or block access. This approach aims to balance security and usability better than static MFA. However, most existing RBA systems rely on centralized data collection and machine learning, leading to privacy concerns, regulatory issues, and poor generalization across heterogeneous environments.

2.3. Federated Learning Essentials

Federated Learning (FL) is a distributed machine learning paradigm that enables multiple clients (devices or organizations) to collaboratively train a shared model without sharing raw data. Only model updates are sent to a central server for aggregation [4].

FL is particularly suitable for authentication because authentication data is privacy-sensitive and naturally distributed across users and domains. It supports cross-domain collaboration while reducing data leakage risks. Nevertheless, applying FL to MFA faces challenges such as non-IID data distributions, temporal concept drift, communication overhead, and vulnerability to poisoning or inference attacks.

Table 1. *Comparison of authentication learning paradigms.*

Paradigm	Privacy Level	Data Handling	Scalability	Key Limitations
Rule-based	High (No ML training)	Manual policies/thresholds	Low; hard to maintain	Fails to capture complex patterns
Centralized ML	Low; high breach risk	Aggregated logs in one server	High, but faces data-transfer bottlenecks	Regulatory compliance issues; single point of failure
Federated Learning	High; local raw data	Local training; shared model updates	High; support cross-domain collaboration	High system complexity; non-IID data challenges

As shown in Table 1, federated learning offers higher privacy and better scalability than centralized approaches, but requires solutions for heterogeneity and system complexity in authentication scenarios.

3. Threat Landscape Against MFA Systems

While Multi-Factor Authentication (MFA) has significantly improved account security compared to password-only authentication, it is not immune to attacks. Modern adversaries continuously adapt their techniques to bypass or exploit weaknesses in MFA deployments. Understanding this evolving threat landscape is essential for motivating adaptive and privacy-preserving authentication approaches.

3.1. Attacks Against Traditional MFA

Traditional MFA, which typically combines passwords with one-time passwords (OTP), SMS codes, or push notifications, remains vulnerable to several common attacks. Phishing attacks trick users into revealing both credentials and second-factor tokens through fake interfaces. Credential stuffing exploits leaked passwords from previous breaches, while SIM swapping allows attackers to intercept SMS-based OTPs by hijacking the victim's phone number [6].

These attacks demonstrate that the effectiveness of MFA strongly depends on the type of factors used and the surrounding security context. Static MFA configurations provide limited flexibility to respond to changing threat conditions.

3.2. Advanced Attacks Bypassing MFAm

More sophisticated attacks have emerged in recent years. Adversary-in-the-Middle (AiTM) attacks position themselves between the user and the legitimate service, proxying the entire session and stealing authentication tokens even after MFA is completed. MFA fatigue (also known as push bombing) overwhelms users with repeated approval requests until they accidentally accept one. Additionally, session hijacking and token replay attacks allow attackers to reuse stolen valid sessions without re-authenticating [7], [9].

Figure 2 illustrates how an Adversary-in-the-Middle (AiTM) attack can bypass MFA by intercepting the authentication flow between the user and the legitimate service.

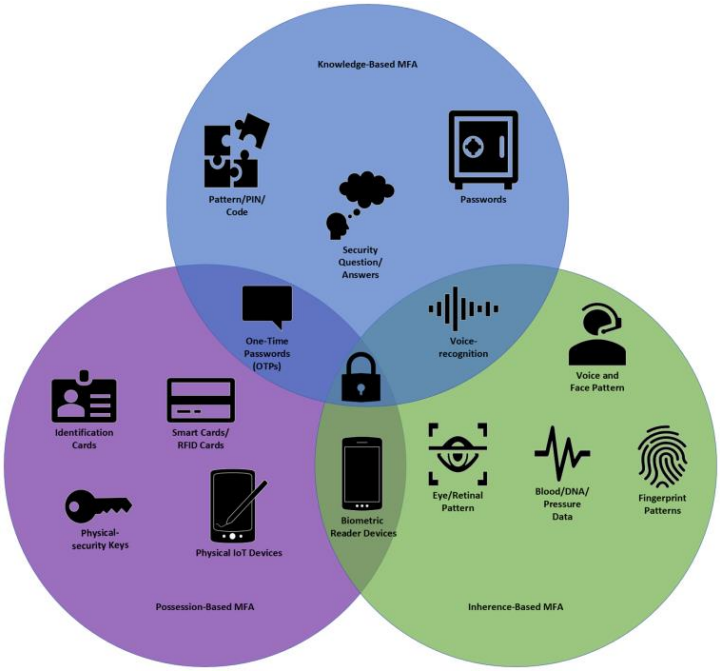

Figure 2. *Illustration of an Adversary-in-the-Middle (AiTM) attack scenario bypassing MFA* [9].

These attacks reveal a fundamental weakness of static MFA: authentication is usually performed only at login time and does not consider ongoing context or behavior after the session begins.

3.3. Implications for Adaptive Authentication

Adaptive and risk-based authentication (RBA) attempts to overcome these limitations by dynamically assessing risk using contextual signals (e.g., location, device), behavioral patterns, and temporal information. Low-risk logins can proceed with minimal friction, while suspicious attempts trigger stronger verification. However, most current RBA implementations still rely on centralized data collection and machine learning, which creates privacy risks, single points of failure, and difficulties in complying with data protection regulations.

3.4. Security and Privacy Challenges in Learning-Based MFA

The use of machine learning in authentication introduces new attack surfaces. Model inference attacks may attempt to recover sensitive information from trained models, while model poisoning attacks may manipulate training data or updates to reduce detection quality. These threats are especially serious in centralized settings where large amounts of authentication data are collected.

Authentication data can also reveal detailed information about user routines, behavior, and organizational structure. As a result, centralized storage and processing raise major concerns related to privacy regulation, data governance, and user trust [9]. These issues reinforce the need for authentication architectures that are both adaptive and privacy-preserving.

3.5. Motivation for Federated and Distributed Approaches

The evolving threat landscape highlights the need for authentication systems that are both adaptive and privacy-preserving. Federated Learning (FL) emerges as a promising direction because it allows collaborative training of risk models across devices or domains while keeping raw sensitive authentication data local. This helps maintain user privacy and regulatory compliance without sacrificing the benefits of collective intelligence [10], [11].

4. Taxonomy of MFA and Authentication Frameworks

Authentication research has evolved rapidly over the past decade, from traditional MFA mechanisms to adaptive, learning-based, and federated approaches. To organize this literature, this section presents a taxonomy of MFA and authentication frameworks from three complementary perspectives: authentication strategy, learning paradigm, and data modality [5].

Figure 3 presents the proposed taxonomy of MFA and authentication frameworks based on authentication strategy, learning paradigm, and data modality.

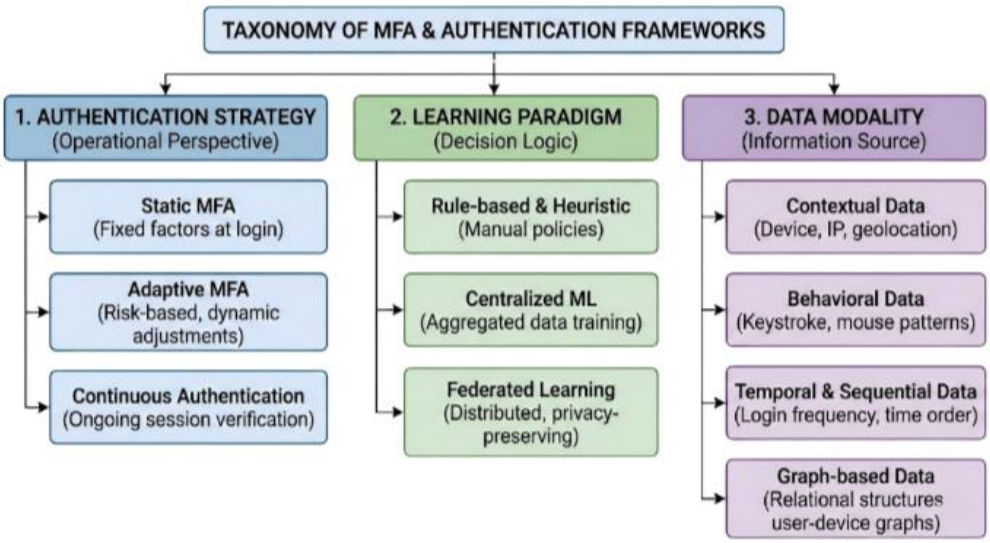

Figure 3. *Taxonomy of MFA and Authentication Frameworks categorized by strategy, learning paradigm, and data modality.*

4.1. Classification by Authentication Strategy

Authentication systems can be categorized by how decisions are enforced. Static MFA requires the same factors for every login, offering simplicity but causing high user friction and limited adaptability to new threats.

Adaptive MFA (Risk-Based Authentication) dynamically adjusts requirements based on estimated risk from contextual and behavioral signals, improving the security-usability balance.

Continuous Authentication verifies identity throughout the session using behavioral biometrics, helping detect session hijacking, but at the cost of increased complexity and privacy concerns.

4.2. Classification by Learning Paradigm

Frameworks differ in how risk estimation is derived. Rule-based approaches use manual policies and thresholds; they are interpretable but fail to capture complex patterns.

Centralized machine learning trains models on aggregated data and achieves higher accuracy, yet raises serious privacy, compliance, and generalization issues.

Federated learning-based approaches train models collaboratively while keeping raw data local. This reduces privacy risks and supports cross-domain collaboration, although it must address non-IID data and system complexity.

4.3. Classification by Data Modality

The effectiveness of authentication systems also depends on the type of data used for identity verification and risk estimation. Different data modalities offer distinct strengths and limitations, and recent studies have begun exploring hybrid combinations to improve overall performance.

Contextual data-based authentication relies on environmental and device-related signals such as IP address, geolocation, device fingerprint, and network characteristics. These features are easy to obtain and impose little burden on users, but they can be spoofed or change frequently.

Behavioral data-based authentication focuses on how users interact with systems, including keystroke dynamics, mouse movements, touch patterns, and usage habits. Behavioral features enable more personalized and continuous authentication but are sensitive in nature and raise significant privacy concerns, particularly in centralized systems.

For example, a hybrid contextual and sentiment-based learning framework has been proposed to capture latent behavioral risk patterns [12]. Similarly, temporal sentiment shifts have been incorporated into federated learning to improve risk detection on non-IID data [13]. Hybrid modality has also been integrated into FL-RBA2 using graph embeddings for relational data, reducing privacy leakage through secure aggregation [13] , [14].

Temporal and sequential data-based authentication models authentication events as time-ordered sequences. Temporal patterns such as login frequency, regularity, and concurrency provide valuable cues for anomaly detection. However, sequence-based models may struggle to capture complex relationships across multiple entities.

Graph-based authentication models represent authentication data as relational structures, for example, user–device or user–service graphs with temporal edges. This representation allows systems to capture both structural relationships and temporal dynamics, enabling richer modeling of authentication behavior. Graph-based approaches are particularly well suited for detecting rare or suspicious interactions but are still underexplored in federated and privacy-preserving settings.

Overall, this taxonomy reveals three main patterns. First, most deployed MFA systems remain static and rule-driven despite known limitations. Second, adaptive and learning-based approaches offer better security and usability but are still largely centralized. Third, federated learning-based authentication is emerging as a promising direction, although it remains fragmented and lacks standardized evaluation principles.

5. Survey of Federated Learning-Based Authentication Systems

Recent research has increasingly leveraged Federated Learning (FL) to address the trade-off between adaptive security and user privacy in MFA systems. This section reviews key FL-based frameworks for risk-based authentication.

A number of studies have explored authentication in federated settings. For instance, a recent survey on IoT authentication using FL classifies methods by architecture and highlights challenges such as communication efficiency, robustness against attacks, and the need for lightweight protocols [15].

5.1. From Centralized Adaptive MFA to Federated Authentication

Large-scale empirical studies have demonstrated that enabling MFA can reduce account takeover risk by more than 99% in enterprise environments [16]. Nevertheless, static MFA and most centralized adaptive systems still face limitations in usability, adaptability to new threats, and privacy protection. Federated Learning has been applied in domains such as IoT and healthcare to train authentication models collaboratively while preserving data locality [15], [17].

5.2. Federated Learning for Risk-Based Authentication

One notable early framework is F-RBA, which applies Federated Learning to risk-based authentication [12]. It uses contextual login features to train local risk models on distributed clients and aggregates updates via Federated Averaging, eliminating the need to share raw user data [10].

Figure 4 shows the general workflow of a federated learning-based risk-based authentication system, from local training on clients to server-side aggregation and risk-based decision making.

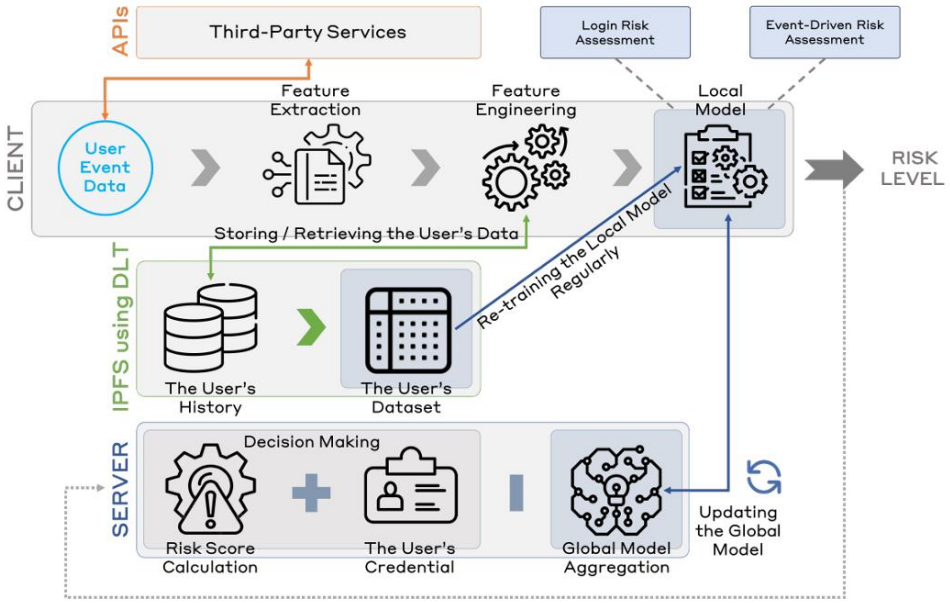

Figure 4. *Workflow of a Federated Learning-based Risk-Based Authentication system* [10].

Its extension, FL-RBA2, addresses non-IID data challenges and incorporates Differential Privacy to enhance protection against inference attacks while preserving detection performance [11], [18]. More recent approaches integrate temporal graph modeling and personalization adapters to better handle concept drift, achieving strong results such as AUC 0.95 on enterprise logs [19] ,[20].

5.3. Key Characteristics and Limitations of FL-Based Authentication Systems

FL-based authentication systems generally keep raw logs local, train risk models collaboratively, and support risk-driven decisions to minimize unnecessary MFA challenges. Privacy is commonly enhanced via secure aggregation and Differential Privacy [21].

Nevertheless, several limitations remain. Authentication data is highly heterogeneous, leading to non-IID issues that affect model performance. System complexity increases when integrating FL with adaptive logic and trust management [10] ,[11]. Many studies prioritize accuracy and privacy metrics but give less attention to usability aspects such as MFA trigger rate and user experience [21]. In addition, robustness against malicious clients and poisoning attacks requires further improvement [22], [23], [24].

In summary, FL offers a promising path for privacy-preserving adaptive MFA, yet current frameworks are still fragmented and would benefit from stronger temporal-relational modeling and standardized evaluation.

6. Modeling Authentication as Temporal and Relational Data: Privacy-Preserving Federated Perspectives

Most traditional authentication systems represent login events as isolated records or short sequences. While simple, this approach fails to capture the inherently temporal and relational characteristics of real-world authentication behavior, where events evolve over time and reflect interactions between users, devices, and services.

6.1. Authentication Logs as Temporal and Relational Structures

Traditional authentication systems typically treat login events as isolated records or short sequences. This simplification fails to capture the temporal and relational nature of real authentication behavior, where events evolve over time and involve interactions among users, devices, and services.

6.2. Temporal Graph Learning for Authentication Risk Modeling

Temporal Graph Learning (TGL) incorporates the order and timing of interactions, enabling dynamic link prediction [25]. In authentication, it estimates the consistency of a login event with historical patterns, supporting better detection of anomalies, long-term drift, and personalized risk scoring. This makes TGL particularly suitable for adaptive and continuous authentication.

6.3. Privacy, Security, and Trust Challenges in Learning-Based MFA

Despite their advantages, learning-based authentication systems raise significant privacy concerns because authentication logs contain sensitive information about user routines and organizational structure. Federated Learning helps by keeping raw data local, but model updates can still leak information through inference attacks, and malicious participants may attempt poisoning. Existing frameworks partially address these issues with secure aggregation and Differential Privacy [25]. System-level authentication mechanisms for federated environments have also been explored [26]. However, many still assume honest-but-curious clients and lack advanced trust management mechanisms [27].

6.4. Proposed Federated Temporal Graph–Based Adaptive MFA Approach

Figure 5 depicts the proposed federated temporal graph-based adaptive MFA framework described in this survey.

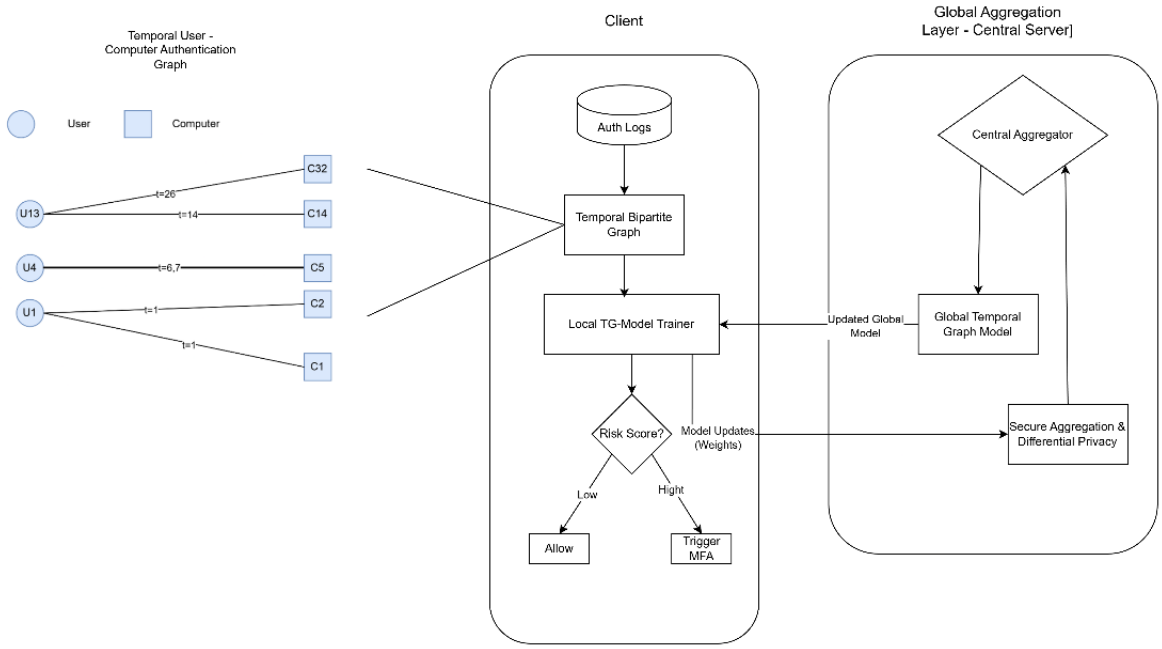

Figure 5. *Proposed Federated Temporal Graph-Based Adaptive MFA.*

To overcome current limitations, this survey proposes modeling authentication as a federated temporal graph learning problem. Each client maintains a local temporal bipartite graph and trains a temporal graph model locally. Only model updates are shared via FL. Risk scores from link prediction drive adaptive MFA decisions — enabling frictionless access for low-risk events and step-up authentication for high-risk ones. The framework operates self-supervised, which suits unlabeled enterprise logs, and can incorporate Differential Privacy for stronger protection.

This direction integrates expressive temporal-relational modeling with federated privacy preservation, addressing key gaps in adaptive MFA.

7. Datasets, Benchmarks, and Evaluation Metrics

The lack of standardized datasets and benchmarks remains a major obstacle in adaptive and federated MFA research. Authentication data is sensitive, personalized, and temporally evolving, limiting sharing

and reproducibility. This section summarizes common datasets, benchmarking practices, and evaluation metrics.

7.1. Authentication Datasets

Studies primarily use three data types. Enterprise authentication logs are highly realistic, recording large numbers of successful logins with contextual attributes. The LANL dataset, containing hundreds of millions of events, is a prominent example [28]. However, these logs usually lack attack labels, leading to unsupervised or self-supervised approaches.

Behavioral biometrics datasets focus on keystroke, mouse, or touch patterns and are useful for continuous authentication, though often limited in scale and collected in laboratory settings [29].

Contextual and risk-based datasets rely on IP changes, geolocation, and device fingerprints [11]. Many are proprietary or synthetic due to privacy constraints, hindering reproducibility.

7.2. Benchmarking Practices in Adaptive and Federated MFA

Benchmarking authentication systems differs fundamentally from benchmarking conventional machine learning models. First, authentication data is inherently non-IID, with strong personalization and domain-specific patterns. Second, security-relevant events are rare, making traditional train–test splits insufficient.

Most surveyed works adopt one or more of the following benchmarking strategies:

- Temporal splitting, where models are trained on historical data and evaluated on future events to reflect real deployment conditions.

- Cross-domain evaluation, in which different organizational units or user groups act as federated clients.

- Cold-start scenarios, where models are evaluated on users or devices with limited historical data.

However, there is no standardized benchmark that jointly evaluates security effectiveness, usability, and privacy under federated settings. As a result, reported performance metrics are often difficult to compare directly across studies.

7.3. Evaluation Metrics

Evaluation of adaptive MFA requires multiple dimensions. Security metrics include AUC, FAR, FRR, and detection rate. Usability metrics focus on MFA trigger rate, friction reduction, and proportion of frictionless logins [21]. FL-specific metrics cover communication overhead, convergence speed, robustness to non-IID data, and privacy budgets. Overall, adaptive MFA should be assessed as a multi-objective problem balancing security, usability, and privacy.

7.4. Discussion and Open Benchmarking Challenges

Current research faces several gaps: lack of large-scale labeled datasets, absence of standardized benchmarks that jointly evaluate security-usability-privacy, and insufficient reporting of usability metrics. Many studies still rely on simplified laboratory settings that do not reflect real enterprise conditions. Progress requires privacy-aware data sharing and more consistent multi-dimensional evaluation practices.

Table 2 summarizes the main research areas in adaptive and federated MFA, highlighting both extensively studied directions and key open research gaps.

Table 2. *Summary of research areas: extensively studied directions and open research gaps*

Research Area	Extensively Studied	Research Gaps
Authentication Strategy	Static MFA and centralized Risk-Based Authentication (RBA).	Continuous authentication and its integration into privacy-preserving, decentralized environments.

Learning Paradigm	Rule-based heuristics and centralized Machine Learning models.	Handling non-IID data distributions and concept drift (evolving user behavior) within Federated Learning (FL).
Data Modality	Tabular contextual data (IP, Location) and basic behavioral sequences.	Temporal Graph Learning to model complex, evolving relational structures between users and devices in a federated setting.
Security & Trust	Basic privacy techniques like Secure Aggregation and Differential Privacy.	Trust management for clients and robustness against malicious participants (poisoning/inference attacks) in FL.
Evaluation & Benchmarking	Technical metrics such as Accuracy, FAR, FRR, and AUC.	Standardized benchmarks and quantitative usability metrics (MFA trigger rate, user friction, and acceptance).

8. Conclusion and Future Work

Research on adaptive multi-factor authentication has grown rapidly with the adoption of machine learning and federated learning. Existing approaches improve security by using behavioral and contextual signals to detect anomalies beyond static credential checks, while federated learning helps preserve privacy by enabling collaborative model training without centralizing sensitive authentication data.

However, several challenges remain. Many systems still depend on domain-specific datasets, limiting generalization across environments. Federated approaches also introduce communication overhead and system complexity, especially at scale, and the lack of standardized benchmarks makes fair comparison difficult. In addition, long-term behavioral evolution and temporal patterns remain insufficiently explored.

Overall, this survey traced the evolution of authentication from static MFA to adaptive, learning-based, and privacy-preserving approaches. While MFA significantly reduces account compromise, static deployments still create unnecessary friction and remain vulnerable to advanced attacks. Adaptive and risk-based authentication addresses part of this limitation, but most existing solutions still rely on centralized data collection, raising concerns about privacy, scalability, and regulatory compliance.

Federated Learning offers a promising direction for adaptive authentication by allowing collaborative learning without direct access to raw authentication logs. Nevertheless, current FL-based frameworks remain fragmented and still need stronger robustness, better usability evaluation, and more standardized benchmarking.

Looking forward, future research should focus on federated authentication models that capture the temporal and relational nature of authentication behavior, such as temporal graph-based learning, while incorporating privacy-preserving and trust-aware mechanisms [24], [30]. Equally important is the development of evaluation frameworks that jointly consider security effectiveness, user friction, and privacy guarantees. Addressing these challenges is essential for transitioning adaptive MFA systems from experimental research to reliable, real-world deployment.

Future research directions include:

- Hybrid FL with temporal graphs and adapters [19] , [20];
- Usability-aware personalization [11], [17];
- Standardized FL-MFA benchmarks [18], [31].

These directions will transition adaptive MFA from research to production deployment [19] , [20] , [27] , [31].

REFERENCES

[1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,” in 2012 IEEE Symposium on Security and Privacy, May 2012, pp. 553–567. doi: 10.1109/SP.2012.44.

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
[3] H. Ramcharan, “The Effective Integration of Multi-Factor Authentication (MFA) with Zero Trust Security,” Open Access Am. J. Math. Comput. Model., vol. 10, no. 1, pp. 1–5, 2025, doi: 10.11648/j.ajmcm.20251001.11.
[4] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-Efficient Learning of Deep Networks from Decentralized Data,” Jan. 26, 2023, arXiv: arXiv:1602.05629, doi: 10.48550/arXiv.1602.05629.
[5] M. Syahreen, N. Hafizah, N. Maarop, and M. Maslinan, “A Systematic Review on Multi-Factor Authentication Framework,” Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 5, 2024, doi: 10.14569/IJACSA.2024.01505105.
[6] S. P. Pote and G. C. Shinde, "A Survey on Adaptive Multi-factor Authentication using Machine Learning," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 2, no. 9, pp. 118-121, May 2022, doi: 10.48175/IJARSCT-3977.
[7] A. K. Wee, E. G. Chekole, and J. Zhou, “Excavating Vulnerabilities Lurking in Multi-Factor Authentication Protocols: A Systematic Security Analysis,” ACM Comput. Surv., vol. 57, no. 11, pp. 1–37, Nov. 2025, doi: 10.1145/3734864.
[8] S. Wiefling, L. L. Iacono, and M. Dürmuth, “Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild,” vol. 562, 2019, pp. 134–148, doi: 10.1007/978-3-030-22312-0_10.
[9] T. Suleski, M. Ahmed, W. Yang, and E. Wang, “A review of multi-factor authentication in the Internet of Healthcare Things,” Digit. Health, vol. 9, p. 20552076231177144, Jan. 2023, doi: 10.1177/20552076231177144.
[10] H. Fereidouni, A. S. Hafid, D. Makrakis, and Y. Baseri, “F-RBA: A Federated Learning-based Framework for Risk-based Authentication,” Dec. 16, 2024, arXiv: arXiv:2412.12324, doi: 10.48550/arXiv.2412.12324.
[11] Y. Baseri, A. S. Hafid, D. Makrakis, and H. Fereidouni, “Privacy-Preserving Federated Learning Framework for Risk-Based Adaptive Authentication,” Sep. 19, 2025, arXiv: arXiv:2508.18453, doi: 10.48550/arXiv.2508.18453.
[12] N. Tran, P. Ta, H. Nguyen, H. D. Nguyen, and A.-C. Le, “Hybrid contextual and sentiment-based machine learning model for identifying depression risk in social media,” Expert Syst. Appl., vol. 291, Art. no. 128505, 2025, doi: 10.1016/j.eswa.2025.128505.
[13] H. D. Nguyen and C. Sakama, “Feature Learning by Least Generalization,” in Inductive Logic Programming, Lecture Notes in Computer Science, pp. 193–202, Feb. 2022, doi: 10.1007/978-3-030-97454-1_14.
[14] L. V. Thinh, " Journal of Science and Technology on Information Security, vol. 24, no. 1, 2025. Federated Trust-Based Authentication for Secure Mobile Cloud Access," doi: 10.54654/isj.v1i24.1113
[15] A. Badhib, S. Alshehri, and A. Cherif, “IoT Authentication in Federated Learning: Methods, Challenges, and Future Directions,” Sensors, vol. 25, no. 24, Art. no. 7619, 2025, doi: 10.3390/s25247619.
[16] L. A. Meyer, S. Romero, G. Bertoli, T. Burt, A. Weinert, and J. L. Ferres, “How effective is multifactor authentication at deterring cyberattacks?” May 01, 2023, arXiv: arXiv:2305.00945, doi: 10.48550/arXiv.2305.00945.
[17] B. D. Deebak and S. O. Hwang, “Federated Learning-Based Lightweight Two-Factor Authentication Framework with Privacy Preservation for Mobile Sink in the Social IoMT,” Electronics, vol. 12, no. 5, Art. no. 1250, 2023, doi: 10.3390/electronics12051250.
[18] R. Aziz et al., “Exploring Homomorphic Encryption and Differential Privacy Techniques towards Secure Federated Learning Paradigm,” Future Internet, vol. 15, no. 9, Sep. 2023, doi: 10.3390/fi15090310.
[19] R. Veiga, C. B. Both, I. Medeiros, D. Rosário, and E. Cerqueira, “A Federated Learning Approach for Authentication and User Identification Based on Behavioral Biometrics,” in *Proc. 41st Brazilian Symp. Comput. Netw. Distrib. Syst.* (SBRC), 2023, pp. 15–28, doi: 10.5753/sbrc.2023.536.
[20] X. Li, Y. Li, H. Wan, and C. Wang, “Enhancing Byzantine robustness of federated learning via tripartite adaptive authentication,” *Journal of Big Data*, vol. 12, Art. no. 121, 2025, doi: 10.1186/s40537-025-01165-y.
[21] M. I. Kamba and A. Dauda, “The Role of Multi-Factor Authentication (MFA) in Preventing Cyber Attacks,” Int. J. Res. Publ. Rev., vol. 6, no. 7, pp. 445–448, Jul. 2025.
[22] T. Le Vinh, H. Thien Tran, H. Trang Phan, and S. Bouzefrane, “Federated Learning-Based Trust Evaluation With Fuzzy Logic for Privacy and Robustness in Fog Computing,” IEEE Access, vol. 13, pp. 137952–137972, 2025, doi: 10.1109/ACCESS.2025.3596093.
[23] Y. Zhang, D. Zeng, J. Luo, Z. Xu, and I. King, “A survey of trustworthy federated learning with perspectives on security, robustness, and privacy,” *arXiv preprint* arXiv:2302.10637, 2023, doi: 10.48550/arXiv.2302.10637.
[24] H. U. Manzoor, A. Shabbir, A. Chen, D. Flynn, and A. Zoha, “A Survey of Security Strategies in Federated Learning: Defending Models, Data, and Privacy,” Future Internet, vol. 16, no. 10, 374, 2024, doi: 10.3390/fi16100374.
[25] E. Rossi, B. Chamberlain, F. Frasca, D. Eynard, F. Monti, and M. Bronstein, “Temporal Graph Networks for Deep Learning on Dynamic Graphs,” Oct. 09, 2020, arXiv: arXiv:2006.10637, doi: 10.48550/arXiv.2006.10637.
[26] Y. Liu, X. Wang, and J. Zhang, “LAFED: A Lightweight Authentication Mechanism for Blockchain-Enabled Federated Learning System,” Future Generation Computer Systems, vol. 139, pp. 346–357, Jan. 2023, doi: 10.1016/j.future.2023.01.015.
[27] T. Ashraf, M. M. Peerzada, M. Abdar, Y. Xie, Y. Zhou, X. Liu, I. A. Gillani, and J. Bashir, “ATR-Bench: A Federated Learning Benchmark for Adaptation, Trust, and Reasoning,” arXiv:2505.16850, 2025, doi: 10.48550/arXiv.2505.16850.
[28] A. D. Kent, “Comprehensive, Multi-Source Cybersecurity Events.” 2015, doi: 10.17021/1179829.
[29] J. Ji, S. Qiu, S. Ye, and X. Liu, “A Hybrid Federated–Incremental Learning Framework for Continuous Authentication in Zero-Trust Networks,” Future Internet, vol. 18, no. 3, Art. no. 154, 2026, doi: 10.3390/fi18030154.
[30] T. L. Vinh, H. T. Tran, H. T. Phan, and S. Le, “Federated learning-based trust evaluation with fuzzy logic for privacy and robustness in fog computing,” *IEEE Access*, vol. 13, pp. 137952–137972, 2025, doi: 10.1109/ACCESS.2025.3596093.
[31] X. Ma, F. Fang, and X. Wang, “Dynamic authentication and granularized authorization with a cross-domain zero trust architecture for federated learning in large-scale IoT networks,” *arXiv preprint* arXiv:2501.03601 [cs.NI], 2025, doi: 10.48550/arXiv.2501.03601.

Trung Kien Pham is currently pursuing the Master’s degree in Computer Science. He received the Bachelor’s degree in Information Technology.
Email: 2591310@student.hcmute.edu.vn. ORCID: https://orcid.org/0009-0003-2811-4659.

Tan Kien Le is currently pursuing the Master’s degree in Computer Science. He received the Bachelor’s degree in Embedded System and IoT Engineering. His research interests include intelligent transportation systems.
Email: 2591309@student.hcmute.edu.vn. ORCID: https://orcid.org/0009-0006-8256-525X.

Vinh Thinh Le completed a Ph.D. at the Conservatoire National des Arts et Métiers (CNAM), Paris, France, in 2017. He is currently working at the Faculty of Information Technology, Ho Chi Minh City University of Technology and Engineering, Vietnam. He has been the author

and co-author of over 20 peer-reviewed scientific articles. He has been actively involved in various research projects and collaborations both nationally and internationally. He is a dedicated educator, committed to fostering a conducive learning environment and advancing the field through research and innovation. His research interests include Trust and Reputation Systems, Security, Mobile Cloud Computing, and the Internet of Things (IoT).

Email: thinhlv@hcmute.edu.vn. ORCID: https://orcid.org/0000-0001-5951-096X.