Analysis of Multi-factor Authentication (MFA) Schemes in Zero Trust Architecture (ZTA): Current State, Challenges, and Future Trends

Yuanyuan Liu (Maxine)
Johns Hopkins University
930 Seymour St.
Vancouver, BC, Canada

ABSTRACT
This research provides a detailed analysis of multi-factor authentication (MFA) in Zero-Trust Architecture (ZTA). It focused the discussion on current practices and critical challenges encountered, sharing some insights into the future direction by finding "gaps." "The field of Cyber security is a constantly changing environment. From the beginning of "trust but verify," it has gradually changed to "always verify, never trust." In this case, MFA becomes a key and effective measure to enhance confidentiality in ZTA. ZTA requires that all entities within the system must verify their identities on an ongoing basis, often using MFA. With the widespread use of telecommuting, cloud services, and the Internet of Things, the demand for identity authentication is also increasing. The MFA uses multiple authentication steps to enhance security and trust in the system. However, implementing and applying MFA in the ZTA environment has not been smooth sailing. Some schemes directly affect the popularity of MFA in their implementation, such as poor user experience, complex integration, and poor scalability. The author first reviewed some of the existing MFA programs to get to the root cause and try to fix the problem. By analyzing these typical cases, best practices are found, and strategies for improvement are proposed. The aim is to promote a balance between ease of use and security in MFA. Finally, through literature review and case studies, as well as the exploration of emerging technologies such as adaptive MFA and zero-knowledge proof, The author explore some new approaches to improve the ease and efficiency of MFA in ZTA systems.

General Terms
Cyber security, Authentication, Zero Trust Architecture, Multi-Factor Authentication, Confidentiality, Scalability, User Experience, Emerging Technologies

Keywords
Zero Trust Architecture, Multi-Factor Authentication, Adaptive MFA, User Experience, password less Authentication, Zero-Knowledge Proof, Cloud Security

1. INTRODUCTION
In today's increasingly popular generative AI, using only "trust but verify" models in the network security environment is rare. More companies and enterprises are adopting the ZTA (Zero Trust Architecture) model and embracing the principle of "always verify, never trust." However, this means constantly authorizing and authenticating every entity that tries to access the system. With the COVID-19 pandemic, telecommuting has become a regular part of work for many people, and cloud environments and the Internet of Things (IoT) are increasingly popular. Unfortunately, this is where confidentiality and availability come into conflict.

As we all know, the core of ZTA is MFA. In other words, the core of access control in this model is the implementation of multiple validation factors to increase the level of trust in the user. This seems to be a model that can significantly improve confidentiality, but it has encountered challenges and obstacles in practical application, such as poor user experience and system integration difficulties. Some have hindered the application of MFA in zero-trust environments.

In simple terms, the core of MFA is to increase users' trust through wording verification. In other words, it is a form of repeated confirmation and verification of authenticity in different ways to reduce the risk of unauthorized access. The mechanism of multiple authentications brings a tedious user experience. This balancing conflict between security and availability can be explained in simplified mathematical formulas. Therefore, to better explain the rationale of MFA in ZTA, readers need to understand the formula used to represent the probability of success in multi-factor authentication:

$$\mathbf{P = 1 - (1 - p)^n}$$

In this simple probability formula, the first assumes that the success probability of single-factor verification is lowercase p and that the MFA contains "n" independent verification steps. The overall success probability of authentication is uppercase P. This formula shows the system's security will improve with increasing verification factors "n." However, as "n" increases, the user experience will naturally suffer, so finding the appropriate "n" value in practice is critical. It can be said that it is the key to helping the MFA achieve a balance between security and user experience.

More profoundly, when the balance point has already been found, how to solve the problem and whether there is a more efficient way in the future are hot topics and urgent issues to be solved by peers.

Therefore, MFA's practical challenges and limitations in a ZTA need to be addressed and discussed in detail.

2. PROBLEM STATEMENT
There is no doubt that the effectiveness of the MFA in promoting confidentiality is widely recognized. However, it is also evident that there are barriers to deployment in the ZTA environment. For example, the complexity of multiple validation steps can be inconvenient for users, leading them to abandon the MFA. In addition, MFA integration technology has a certain complexity. However, the reality is that enterprises often have different platforms to operate and

manage, and integrating and expanding between these systems is an inevitable technical problem. Therefore, the primary purpose is to analyze this situation in depth, identify the main obstacles, and propose some MFA strategies without sacrificing user experience while maintaining system performance.

2.1 Sample list of research questions

-What are the current MFA schemes implemented in the zero-trust architecture, and how do they work?

-What are the main challenges these MFA solutions face regarding security, user experience, scalability, and integration?

-What strategies can improve the effectiveness and usability of MFA in a zero-trust environment?

3. RESEARCH METHOD

To achieve the expected results and achieve the research objectives, three main research methods will be adopted:

3.1 Systematic literature review

Review of 18 academic papers and industry reports following the plan. Through a literature review, the author put forward an understanding of the current situation of MFA and tried to identify the challenges faced by MFA.

Emerging technologies are viable solutions to resolve the conflict between availability and confidentiality. To devise solutions, the researcher conducted an in-depth review of some papers involving zero-knowledge proof and password-less authentication techniques. These techniques simplify the authentication process while maintaining a high level of confidentiality.

3.1.1 Key point 1: Balance confidentiality and availability

In the book "Multifactor Authentication," Progress in User Authentication, by D. Dasgupta, A. Roy, and A. Nag, A systematic explanation of the principles and progress of MFA, as well as the challenges encountered when security and usability are not compatible, is presented [1].

Several studies have shown that MFA technology is a solution created to solve the security vulnerabilities of traditional single-factor authentication. However, some researchers have found that the low adoption rate of MFA is inevitable, and there is a widespread avoidance phenomenon in mandatory use [2]

This research surveyed 18 existing literatures on MFA and found that 94% (17/18) mentioned poor usability or user experience. Thus, one of the biggest challenges in implementing MFA is balancing confidentiality and availability.

3.1.2 Key point 2: Zero-Knowledge proof in MFA

Saeid Ghasemshirazi, Ghazaleh Shirvani, and Mohammad Ali Alipour, in their paper Zero Trust: "Applications, Challenges, and Opportunities," note that combining emerging technologies such as artificial intelligence and machine learning significantly improves the effect of zero trust. This solution does not rely on traditional cryptography and can be used in environments with high-security requirements [3], providing a more dynamic and flexible solution for network security.

Other studies have also shown that the AGZKP-AP protocol can help users set privacy through the ZKP method [4]. This means that users can implement name authentication. In other words, this design can balance resource utilization (availability) and privacy protection (security). The researcher follows Adenubi's paper on the adaptive Group-based Zero Knowledge Proof-Authentication Protocol (AGZKP-AP) in Vehicular Ad Hoc. The AGZKP-AP scheme in Networks is verified in practical experiments [4]. The author follows their scheme verification and finds that specific technical means, such as network broadcast, can be used to revoke the user's permission when malicious behavior is detected. Therefore, the scheme's effectiveness in preventing malicious users from accessing is verified.

3.2 Case Study Analysis and Result

The challenge of MFA is more in the actual deployment phase. Therefore, analyzing actual deployment cases is critical to understanding the exact difficulties. For example, when studying the case of MS Azure AD and Cloud deployments, this research examined the reasons for their obstacles and summarized their successful experiences.

3.2.1 Priority 1: Phased deployments

Microsoft Azure Active Directory (MS Azure AD) is widely used. Due to its seamless single sign-on technology in authentication, it has high reference value in studying the phased deployment of MFA. Therefore, the author uses the case study of D. Subbarao et al. to compare the experimental results and provide some technical lessons for organizations that must deploy on a scale.

To verify feasibility, the researchers used Visual Studio 2019. NET Core SDK will implement and validate the transformation in this case. In the past, authentication protocols such as SANL2.0 or WS-Fed typically separated the authentication method from the functionality and generally did not handle user credentials directly. However, in AZURE AD, the login process is managed to allow users to use multiple authentication methods. These numerous authentication methods also allow non-password forms of facial recognition and biometrics. From the results of the experiment, Azure AD blocks or raises authentication requirements when user accounts log in from untrusted locations. When researchers upgrade from Visual Studio to MS Authentication Library from Azure Active Directory Authentication Library, they can better support MFA. Ensure the security of the SAML protocol request response.

3.2.2 Priority 2: Cloud deployments

In Cloud deployment, the major service providers and their products include Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. Each cloud platform has its characteristics and meets the needs of different use cases. For example, MS Azure works with Microsoft's infrastructure and is, therefore, more appropriate for organizations with a lot of Microsoft infrastructure. However, organizations with complex security needs may prefer AWS. For more cost-effective organizations, GCP is often a better fit.

The researchers compared AWS, GCP, and Azure against publicly available data. Table 0 below shows the differences and similarities in price, deployment, availability, and more.

Table 0 MS Azure vs. AWS vs. GCP comparative analysis

Service	MS Azure	GCP	AWS
Launching	2010	2008	2006
Deployment Models	Azure AD	Identity & AccessControl	IAM
PaaS	Azure APP Service	Google App Engine	AWS Elastic Beanstalk
Identity & Access Management	MS Entra ID, Azure RBAC	Cloud IAM, Identity Platform	AWS IAM, AWS DS
Protection	Firewall, MS Defender	Cloud Amor	Firewall & AWS Shield
Data	Kdy Vault & Certificates	Cloud KMS & Cloud HSM	AWS KMS & Certificate Manager

The author uses MS Azure, which is more equal in all aspects, as an example to analyze the effectiveness of account protection in the business environment when enabling MFA in the cloud environment.

In a 2023 study by Meyer et al., using the baseline multiplication method and manual account review, dedicated MFA was found to be superior to SMS verification in terms of protection effect [3]. Studies have also shown that MFA-enabled accounts can achieve 99.99% security and effectively resist unauthorized access [5]. Other studies have shown that even in more extreme cases where the credentials are known to have been compromised, MFA-enabled accounts are 98.56% less risky [6].

Since it is difficult to observe the actual incidence of attack events directly, the author simulated some compromised accounts as a benchmark sample in the experiment and used the benchmark multiplication method to estimate the number of compromised accounts in a large Azure AD user base.

The results support the above studies, and MFA can significantly reduce the risk of account breaches.

3.3 Security and applicability analysis of different MFA schemes

From the above literature and cases, it is not difficult to see that implementing MFA in ZTA does face various challenges. In particular, the security and applicability of different multi-factor authentication schemes differ significantly. To analyze the advantages and disadvantages of these solutions more comprehensively, the author compares several standard solutions and shows their performance in various aspects.

Table 1. Comparative Analysis of Various MFA Solutions

MFA Solution	Security Level	User Experience	Cost	Scalability	Suitable Scenarios
Password + SMS Verification	▲	●	■	●	Suitable for small to medium-sized businesses with moderate security requirements.
Biometric Authentication	●	●	△	▲	Ideal for high-security environments like financial institutions and government agencies.
Hardware Tokens	○	□	●	▲	Suitable for high-risk sectors requiring stringent security, e.g., defense or healthcare sectors.
Adaptive MFA	●	●	●	●	Best suited for enterprise applications requiring flexible, behavior-based security adjustments.
Zero-Knowledge Proof Authentication	●	●	▲	▲	Suitable for environments requiring strong privacy protection and data sensitivity, such as healthcare and cloud storage.

○	Very High	●	High
▲	Moderate	△	Moderate to High
□	Low to Moderate	■	Low

As shown in Table 1 above, researchers select five major MFA schemes today and show their applicability in different scenarios, such as comparing user experience, cost, and scalability.

3.3.1 Data support and analysis of Table 1

3.3.1.1 Password + SMS authentication:

According to the data in [7]and [8], although this method has some security, it is still limited because SMS can be intercepted or spoofed. However, the solution has user experience and cost advantages and is suitable for small and medium-sized enterprises with relatively low-security requirements.

3.3.1.2 Biometrics:

Research shows that [9] a biometric identification scheme can effectively improve user convenience and safety. Still, there will be problems with recognition performance changes due to environmental changes and sample aging. Although adaptive biometrics systems are already trying to cope with these changes, such as dynamically adjusting the sampling, further research is still needed into persistent authentication methods for mobile and wearable devices. It follows that it needs to evaluate the feasibility of large data sets and achieve application scalability. Therefore, the author believes that implementation cost and system integration requirements are slightly higher, and it is more suitable for scenarios with higher security requirements, such as financial institutions or governments.

3.3.1.3 Hardware tokens:

Due to the increasing popularity of the Internet of Things (IoT), the certification requirements for security devices are constantly increasing. However, these devices often rely on token authentication, and several papers have addressed the topic of token leakage attacks. For example, the MCU-Token proposed in Yue Xiao et al. 's paper [10], a secure hardware fingerprint framework, can provide protection even if the private key is breached. Bind tokens specific requests through hardware fingerprints and add obfuscation data to prevent machine learning attacks. It follows that while hardware tokens perform well in high-risk environments, the expense and

maintenance costs of the device are still the limiting conditions. In particular, the problem of popularization in some large enterprises is particularly prominent.

3.3.1.4 Adaptive MFA:

Research [9] shows that adaptive MFA can dynamically adjust authentication steps based on user behavior to improve user experience and is suitable for enterprises that need to adjust security flexibly.

3.3.1.5 Zero-knowledge proof certification:

The emerging technology zero-knowledge proof performs well in high-security environments, especially in privacy protection [2]. However, this technology is still in the promotion stage, and its application cost and compatibility still need to be further optimized.

3.3.2 Conclusion and result of analysis

Based on reviewing the literature above and analyzing the cases in article 3.2, some complex MFA schemes can significantly improve security, such as biometrics and hardware tokens. However, due to the added burden and accurate cost of implementation for the user, especially when implementing the deployment in a relatively large enterprise, the applicability of the situation is lower. In contrast, some seemingly more basic MFA schemes, such as password + SMS authentication, despite relatively low security, are still suitable for use in environments with low-security requirements due to friendly user experience and low cost.

The above comparison shows that choosing the suitable MFA scheme depends on the specific application scenario and security requirements. In a ZTA environment, the ideal solution is to balance security and user experience.

4. GAP ANALYSIS RESULT AND FUTURE TREND EXPLORATION

After literature reviews and case studies, the researcher can identify gaps. Therefore, some solutions will be explored, such as password-less authentication, adaptive MFA, and zero-knowledge proof. The author examines how new technologies can improve security while striking a good balance between confidentiality and availability.

Three key trends that are likely to affect MFA development in the ZTA environment

4.1 Result 1: Focus on Adaptive MFA

A smarter MFA that dynamically adjusts authentication requirements based on user behavior and reduces unnecessary verification steps. A-MFA's significant advantage is that it can effectively balance the user experience with improved security, but it is imperfect. There are also some challenges in practical applications, such as data privacy, storage overhead, and the training and updating of machine learning models.

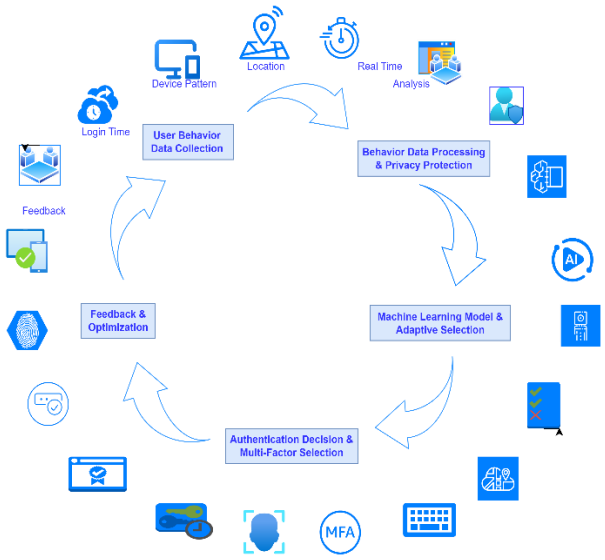

Fig 1: Adaptive MFA System Framework

Fig 1 shows the data flow and interaction between modules in the Adaptive MFA system and how the various components work together to ensure security and adaptability.

4.1.1Data Privacy and Security:

Collecting and analyzing large amounts of user behavior data is the foundation of adaptive MFA. This data protects but is not limited to geographic location, device usage patterns, login times, etc. However, this is sensitive data that involves user privacy. As a result, using this data may raise risks and some compliance issues. For example, when implemented by medical institutions, they face the risk of data leakage and the compliance problem of HIPAA privacy protection.

4.1.2 Computing and storage costs and overhead:

Implementing A-MFA requires analyzing and processing user behavior data, often in real time. This undoubtedly means higher computing power and storage resources. Therefore, for some large enterprise application environments, increasing the cost and complexity of the infrastructure can hinder the implementation of this strategy. On the other hand, the resources of some IoT devices are limited, and A-MFA may cause their system performance to degrade.

4.1.3 ML model training and updating

When A-MFA analyzes and identifies user behavior patterns, it relies on ML models. Therefore, the ML models must constantly learn new patterns to adapt to environmental changes. This is especially important when faced with sizeable real-time data processing requirements. In addition, some new and targeted attacks also need to be quickly responded to. Then, updating swiftly is also an ongoing challenge.

4.1.4 Future A-MFA Trends

Given the current situation, the future trend of A-MFA is likely to be towards becoming more intelligent and dynamic to build more easily integrated protection mechanisms, such as multi-modal biometric identification (such as face and fingerprint) technology combined with continuous authentication technology.

In addition, behavioral anomaly detection and updated ML learning models can automatically adjust recognition

parameters when new attacks are detected when faced with more complex security threats. These techniques can improve the ability to defend against copycat attacks.

For example, technologies such as multimodal biometrics, behavioral anomaly detection, and persistent authentication can be combined to enhance the system's defenses against behavioral mimicking attacks, helping A-MFA face more complex challenges while creating A seamless authentication experience for users.

4.2 Result 2: Focus on Password-less authentication.

In a password-less Zero Trust environment, MFA is seamlessly integrated with biometrics or hardware tokens, which provide an additional layer of verification [11]. Biometrics and FIDO2, for example, do not use passwords. This technology, which utilizes biometric data and encryption methods, is particularly well suited to protect against phishing attacks and reduce the risk of password theft.

Password-less authentication technology has more advantages in preventing phishing attacks and reducing the risk of Password theft [12]. For example, FIDO2 can reduce the operation steps and the uniqueness of separate biometric characteristics and storage methods (the key is stored in the device, and the authentication information is stored in the server).

More attention will be paid to protecting user privacy in industries with high-security requirements, such as finance and healthcare. Therefore, password-less technology is likely to replace the traditional Password system.

4.3 Result 3: Focus on Zero-knowledge proof.

Users can verify their identities without exposing too much sensitive information by integrating zero-knowledge proof into MFA systems. As shown above, the best practice for anonymous authentication allows the vehicle to access the network without revealing its identity [13]. This can protect users' privacy and avoid being tracked.

In the future, as artificial intelligence will enhance the detection of abnormal behavior, ZKP could lead to more efficient distributed verification.

5. THE OTHER RESULTS AND ADVICE

The researchers comprehensively assessed MFA's current situation and challenges in the ZTA environment. At the same time, it proposes some improvement strategies and tries to predict MFA's development trend. Therefore, the author makes some suggestions based on the evaluation and shares some understanding of future research directions.

5.1 Result 4: Expanded Evaluation

The advantages and disadvantages of the MFA system in the ZTA environment are apparent, and the evaluation is as follows:

5.1.1 Advantages:

First, significantly improved security. When the user environment changes dynamically, MFA can continuously verify and combine multiple authentication factors such as biometrics, dynamic passwords, and hardware tokens. This means that the MFA can effectively prevent unauthorized access in the ZTA, thus ensuring access is limited to authorized people.

Second, the MFA's flexibility in defining the level of security according to the organization's needs can provide tighter protection.

5.1.2 Weaknesses:

First, MFA affects the user experience, and complex verification processes can cause inconvenience to users.

Secondly, there are problems of response delay and operation and maintenance costs under multiple verification methods. Resource constraints and load balancing conflict challenges.

Third, availability is entirely dependent on the device and the network. Once the network is disconnected or the device is not in a state, authentication cannot be carried out, and it may also lead to business interruption.

5.1.3 Comment

All in all, the following recommendations should be followed in future implementation to enhance the effectiveness of MFA in ZTA by improving convenience and combining new technologies.

5.2 Result 5: The Future Scope of the Idea

Several specific recommendations will be made to improve the MFA

5.2.1 Adaptive MFA is actively introduced to reduce verification and adjust validation requirements dynamically.

Some blockchain-based, adaptive multi-factor authentication (A-MFA) selection frameworks could be considered. In this way, you can maintain some flexibility and improve authentication security. For example, the experiments conducted by Xu Yanbin et al. showed that compared with random and optimal cost selection methods, adaptive selection methods performed better in terms of safety [14] Similar experiments dynamically select authentication factors by adjusting the weights of different devices and media combinations to enhance anti-aggression. This result of the Xu Yanbin et al. experiment is shown in Figure 2. It is difficult for an attacker to identify any selection pattern, and the adaptive selection method is superior to other methods in all trigger events [14]. Therefore, the research propose an adaptive multi-factor authentication strategy combined with LRaft (a formula model for fast security authentication) and a blockchain-based authentication framework that balances applicability and provides flexible, effective, and secure authentication solutions.

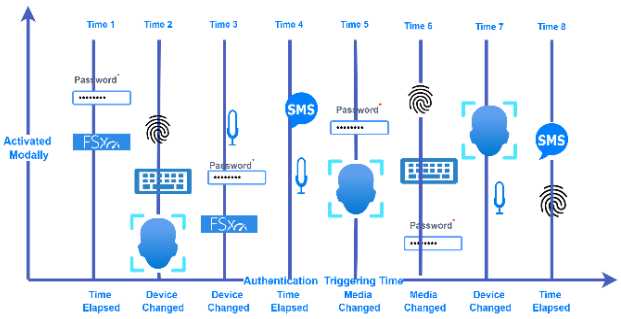

Fig 2 Multiple modality selections under diverse triggering events [9].

Given the gap mentioned in 4.1 above, the A-MFA should also make the following arrangements: pay attention to data privacy protection, optimize computing and storage resource allocation,

and improve the adaptability of machine learning models. For example, strict data protection measures ensure the privacy and compliance of user behavioral data. In addition, more efforts should be made to select storage strategies and improve the rapid updating ability of ML models.

5.2.2 Actively promote biometrics in cloud environments, allowing password-less authentication to replace passwords. Examples include FIDO2 standards and hardware tokens.

As Casey, Manulis, Newton, Savage, and Treharne have shown in their research, passwordless authentication methods (FIDO2 standard and hardware tokens, etc.) combined with biometrics and encryption can effectively prevent the risk of credential theft and phishing attacks and provide users with a more convenient and secure authentication experience [15][16].

Therefore, considering the future of cloud security, this recommendation should be one of the critical pillars for enterprises and users to build a more efficient security protection system.

5.2.3 Combine multi-modal biometrics with zero-knowledge proof technology in high-security enterprise environments.

Because ZKP supports the dynamic balance of privacy protection, the level of privacy can be set according to the demand, which can be a more efficient use of resources and effectively reduce latency. Therefore, combining ZKP with multimodal biometrics will be ideal for high-security enterprises. In addition, as shown in the previous case analysis, the distributed permission control and revocation mechanism can identify some malicious users' access and expose the user's identity.

Therefore, this recommendation's lower latency and higher security suit organizations with high real-time authentication requirements.

5.3 Result 6: Optimization Direction

In addition to the above recommendations, a particular direction that needs to be proposed is the application and exploration of MFA in AI technology and scalability.

5.3.1 AI real-time analysis

AI can be used for real-time analysis of user behavior and location. This allows you to automatically adjust the validation lead without sacrificing the user experience. The ultimate balance between security and availability.

-Implementation scenario tips:

Employees in different regions can log in from multiple locations in a multinational or cross-regional corporate environment. Companies can drive AI to detect employee login anomalies, such as abnormal login times or locations. However, only trigger additional verification steps when necessary. AI differentiates risk levels for different scenarios. For routine operations in low-risk scenarios, seamless access can be provided, while for suspicious behavior in high-risk scenarios, AI can simultaneously enhance protection.

- Implementation methods and advantages

First, collect user habits and behavior data, including login habits, mouse movement patterns, and keystroke dynamics. The necessary data analysis is then conducted using AI models. Finally, machine learning techniques, such as anomaly detection or cluster analysis, identify anomalies that deviate from typical user behavior.

This method can reduce unnecessary authentication steps, thereby improving the user experience. At the same time, it can focus on high-risk abnormal behavior events and improve the utilization efficiency of system resources.

5.3.2 AI-driven adaptation

AI-driven adaptive authentication can solve the problems of efficient scaling and maintaining stability. A multi-level MFA system can help large enterprises maintain stability and availability amid high traffic, especially as traffic surges and the number of MFA users increases.

- Problem solving scenario.

In large enterprises, a sudden surge in traffic and high concurrent user demand during peak hours or certain times can overwhelm traditional systems. AI-driven mechanisms are expected to dynamically allocate resources and adjust authentication protocols to maintain performance, thus achieving the role of preventing such bottlenecks, preventing downtime, and allowing the enterprise to file the system.

- Implementation methods and examples

One direction is to develop a multi-level authentication strategy based on AI algorithms while integrating predictive analytics techniques. This way, tasks can be prioritized based on risk assessment, trend analysis results can be obtained in advance, and system resources can be expanded using the predicted traffic pattern.

For example, on Christmas Eve or during Black Friday sales, banks or financial institutions can deploy AI-powered adaptive multi-factor authentication in advance. This arrangement can pre-select enhanced authentication agreements to help financial institutions cope with significantly increased trading volumes.

5.3.3 MFA combined with ZKP

For high-security certifications such as hospitals or vehicles, MFA combined with ZKP technology can further protect privacy during the verification process and achieve security without disclosing user identity information. The study above shows that it is an efficient and balanced choice.

-Implementation scenario tips:

The combination of MFA and ZKP is a viable and innovative solution for high-security environments in the medical field and autonomous vehicles.

For example, healthcare workers should be certified when they are sensitive to patient data. At the same time, ensure that their identity information is utterly inaccessible to unauthorized people. In addition, the verification of autonomous vehicles in the network can also adopt this method. Verifying secure communication between these networked vehicles can protect the driver's anonymity.

- Implementation methods and advantages

ZKP can be combined with biometric patterns, such as face recognition or fingerprint recognition, to verify user credentials through the ZKP protocol without disclosing sensitive information. This arrangement increases security while ensuring compliance with GDPR and HIPAA privacy regulations.

One obvious benefit is increased privacy and security while reducing the risk of social engineering attacks and the likelihood of phishing attacks.

To sum up, the future MFA optimization direction in ZTA should focus on AI (application intelligence and scalability) to

explore flexibility and to create a more efficient authentication mechanism to balance security and availability

6. CONCLUSION

Implementing MFA faces both user and technical challenges in practical applications. However, there is no denying that MFA is the core of ZTA. One shortcut for enterprises to enhance security is to reduce the user abandonment rate of MFA. By applying and improving some innovative technologies, such as adaptive MFA, password-less authentication, and zero-knowledge proof, the practicality and scalability of MFA will be enhanced.

This study recommends four directions for maximizing the effectiveness of multi-factor authentication (MFA) in zero-trust architecture (ZTA) in the future.

First, fully utilize the power of artificial intelligence (AI). Please set up a real-time data flow state adjustment and verification mechanism to promote the system of medium-sized enterprises' greater flexibility and adaptability, improve responsiveness, and continue to learn and adapt to new models, making it more adaptable to new threats and challenges.

Secondly, cloud solutions should meet the increasing number of users and device diversification enterprises face as they scale, ensuring that the MFA has good scalability and can meet users' growing needs. A modular design approach is recommended to synchronize the solution with enterprise-scale expansion while facilitating integration with new technologies.

In addition, multimodal systems are being actively explored to combine face, voice, and fingerprint recognition. These systems should be integrated with behavioral analysis, enabling robust authentication capabilities and a seamless, secure user experience.

Finally, new systems need to be interoperable with emerging standards. It is essential to keep up with industry standards such as FIDO2 and ensure the system's multi-platform or device compatibility. Still, it is also vital to develop APIs that integrate seamlessly with existing infrastructure.

Together, these optimization strategies can help MFA better balance security and user experience, solve today's challenges, and lay the foundation for a brighter and more efficient certification framework.

7. REFERENCES

[1] D. Dasgupta, A. Roy, and A. Nag, "Multi-Factor Authentication," in Advances in User Authentication, Infosys Science Foundation Series, Springer, Cham, 2017, pp. 45-68. DOI: 10.1007/978-3-319-58808-7_5

[2] Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019). Evaluating user perception of multi-factor authentication: A systematic review. arXiv preprint arXiv:1908.05901

[3] Ghasemshirazi, G. Shirvani, and M. A. Alipour, "Zero Trust: Applications, Challenges, and Opportunities," arXiv preprint, 2023. DOI: 10.48550/arXiv.2309.03582.

[4] Adenubi, Adeola & Oduroye, Ayorinde. (2023). "ZERO TRUST NETWORKS: A PARADIGM FOR PASSWORD-LESS AUTHENTICATION IN THE MODERN CYBERSECURITY LANDSCAPE."

[5] Microsoft: 99.9% of compromised accounts did not use multi-factor authentication. https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factorauthentication/, 2020.

[6] Ariel F. Pomputius. A Review of Two-Factor Authentication: Suggested Security Effort Moves to Mandatory. Medical Reference Services Quarterly, 37(4):397–402, 2018.

[7] Roger Piqueras Jover. 2020. Security analysis of SMS as a second factor of authentication. Commun. ACM 63, 12 (December 2020), 46–52.

[8] Zukarnain ZA, Muneer A, Ab Aziz MK. Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges. Symmetry. 2022; 14(4):821. https://doi.org/10.3390/sym14040821

[9] Riseul Ryu, Soonja Yeom, David Herbert, Julian Dermoudy,The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction, ICT Express,Volume 9, Issue 6,2023,Pages 1183-1197,ISSN 2405-9595, https://doi.org/10.1016/j.icte.2023.04.003.

[10] Xiao, Yue, et al. "From Hardware Fingerprint to Access Token: Enhancing the Authentication on IoT Devices." arXiv preprint arXiv:2403.15271 (2024)

[11] D. Subbarao, B. Raju, and F. Anjum, "Microsoft Azure Active Directory for Next Level Authentication to Provide a Seamless Single Sign-On Experience," Applied Nanoscience, vol. 13, pp. 1655-1664, 2023. DOI: 10.1007/s13204-021-02021-0.

[12] Xu, Yanbin, Jian, Xinya, Li, Tao, Zou, Shuang, Li, Beibe i, Blockchain-Based Authentication Scheme with an Adaptive Multi-Factor Authentication Strategy, Mobile Information Systems, 2023, 4764135, 13 pages, 2023. https://doi.org/10.1155/2023/4764135

[13] Gartner (2019). Hype Cycle for Identity and Access Management Technologies, 2019.

[14] Casey, M., Manulis, M., Newton, C.J.P., Savage, R., Treharne, H. (2020). An Interoperable Architecture for Usable Password-Less Authentication. In: Saracino, A., Mori, P. (eds) Emerging Technologies for Authorization and Authentication. ETAA 2020. Lecture Notes in Computer Science(), vol 12515. Springer, Cham. https://doi.org/10.1007/978-3-030-64455-0_2

[15] World Economic Forum: Passwordless authentication: The next break-through in secure digital transformation. http://www3.weforum.org/docs/WEF Passwordless Authentication.pdf (2020)

[16] M. Belotti, N. Božić, G. Pujolle and S. Secci, "A Vademecum on Blockchain Technologies: When, Which, and How," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3796-3838, Fourthquarter 2019, doi: 10.1109/COMST.2019.2928178.

[17] Xu, Y., Meng, Y. & Zhu, H. An Efficient Double-Offloading Biometric Authentication Scheme Based on Blockchain for Cross Domain Environment. Wireless Pers Commun 125, 599–618 (2022). https://doi.org/10.1007/s11277-022-09567-

[18] "How effective is multifactor authentication at deterring cyberattacks?" arXiv preprint, 2023. DOI: 10.48550/arXiv.2305.00945.