Design and Evaluation of a Multi-Domain Adaptive Multi-Factor Authentication Framework for Holistic Cybersecurity Reinforcement

S. Kannadhasan[1], Pilli Lalitha Kumari[2], Yuvarani R.[3], S. Venkatesh[4], Suniesh P.[5] and N. Shirisha[6]

[1]*Department of Electronics and Communication Engineering, Study World College of Engineering, Coimbatore - 641 105, Tamil Nadu, India*

[2]*Department of Computer Science and Engineering Visakha Institute of Engineering & Technology, 88th Division, Narava Visakhapatnam - 530027 Andhra Pradesh, India*

[3]*Department of Management Studies, Nandha Engineering College, Vaikkalmedu, Erode, Tamil Nadu, India*

[4]*Department of Computer Science and Engineering, J. J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India*

[5]*Department of CSE, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India*

[6]*Department of CSE, MLR Institute of Technology, Hyderabad, Telangana, India*

Keywords: Multi-Factor Authentication, Cybersecurity, Adaptive Security, Biometric Spoofing Prevention, Quantum-Resistant Authentication.

Abstract: In the era of advanced cyber-attacks and the growing digital inter-connectivity the traditional authentication methods do not guarantee a high security level. This research introduces an advanced multi-factor authentication (MFA) framework featuring resiliency, user-centricity, and adaptiveness, for modern cyber security systems hardening. The framework leverages biometric anti-spoofing methods, light-weight IoT-friendly protocols, and AI-powered behavioral analytics to mitigates usability limitations, phishing risks, and post-quantum attacks. Then a hybrid solution which combines MFAaaS with the ability to adapt to regulatory compliance is proposed to address the weaknesses of the current MFAaaS systems. We also conduct real-world simulations and case studies to demonstrate the effectiveness of the proposed model in enterprise, healthcare and mobile environments. The results show that the context-based and adaptive MFA system effectively improves security posture without sacrificing access and usability. This study not only closes the void between academic investigation and practice, but also produces a road map for everywhere-available strong authentication in the future cyber world.

1 INTRODUCTION

With the rise of digitalisation, increasing dependence on online services and interconnected systems have made strong cyber security more important than ever before. There are increasing threats from cyber-attack on system vulnerabilities as well as human vulnerabilities, such as phishing, identity theft and social engineering. Legacy authentication methods – which are based primarily on just a single factor, including passwords – have not been able to adequately protect against multifaceted threats such as these. Multi-Factor Authentication (MFA) has been developed as a strong application to authenticate the user by using some knowledge factors (password), possession factors (ID devices) and inherence factors (biometric or behavior).

But despite its advantages, traditional MFA solutions have significant drawbacks such as being inconvenient for users, not being scalable to IoT type of environments, not being able to respond to new emerging threats such as SIM swaps and deepfake hacks, and becoming vulnerable to quantum compute attacks. There are also more significant barriers to establish the use of MFA in practice, including lack of standardised regulation, lack of user understanding, and integration issues in legacy systems.

In this paper, we present the next-generation MFA framework, which not only overcomes the shortcomings of MFA solutions but also

Kannadhasan, S., Kumari, P. L., R., Y., Venkatesh, S., P., S. and Shirisha, N.
Design and Evaluation of a Multi-Domain Adaptive Multi-Factor Authentication Framework for Holistic Cybersecurity Reinforcement.
DOI: 10.5220/0013859400004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 1*, pages 151-157
ISBN: 978-989-758-777-1

revolutionizes the way of digital identity verification. Key to this is a focus on intelligent security models driven by artificial intelligence (AI), next-gen quantum-resistant cryptographic algorithms, and privacy preserving decentralized models. This model hopes to provide a scalable and well-prepared MFA approach, and to form a stronger defence framework across wide range of digital environments by seating at its heart usability and resilience.

2 PROBLEM STATEMENT

Description Although Multi-Factor Authentication (MFA) has been heralded as key to the improvement of cybersecurity, current MFA deployments are typically flawed by severe limitations that drastically reduce its security and usability. Existing technologies find it hard to achieve a good tradeoff between security and user convenience, and commonly present usability friction and low compliance. Furthermore, the aforementioned MFA solutions are not effective in IoT ecosystem and are not adaptable to the resource-limited environment and challenging for preventing advanced threats including phishing, biometric spoofing, and SIM-swapping attacks. The advent of quantum computing will further amplify the demand for more secure means of authentication, as traditional cryptographic approaches may be rendered useless. Moreover, uneven implementation of user control requirements and the complexity of MFA integration into legacy and hybrid cloud environments limit its general applicability. The urgency of MFA mechanisms, push us in the direction of deploying, sensing and evaluating/ managing a next generation MFA framework, which would be adaptable, user centric, cost sensitive, capable of withstanding, current/intelligence threat.

3 LITERATURE SURVEY

Authentication methods have evolved at the very heart of cyber security and fundamental changes have been driven in the past couple of years. Traditional password-based scheme has been widely criticized due to its vulnerability to the brute force attack, credential spilling, phishing (Bhargava & Wu, 2021). Therefore, the multi-factor authentication (MFA) is offered as a more secure platform where the users are asked for more than one type of evidence of identity (eg a password, and a token, or biometric characteristic) (Abid & Ahmad, 2023).

Yet MFA remains far from universally adopted, primarily due to its usability difficulties. Researches have shown that MFA systems are usually perceived as inconvenient by users which influence the compliance and user satisfaction negatively (Alotaibi & Furnell, 2021; Ferreira & Antunes, 2021). This problem is even more prominent in fields that access must be simple such as the health sector and mobile service (Saleh & AlZain, 2024).

Recent developments have been toward to improve MFA using biometric authentication. Though biometric identifiers enhance security, they also raise novel risks including spoofing and deepfake attacks (Barni & Dini, 2022; Jang & Kim, 2024). To mitigate these challenges, liveness detection and hybrid biometric approaches enhancing resiliency have been proposed.

Phishing and SIM-swapping continue to pose a threat to MFA systems using SMS based onetime passwords (Ahn et al., 2022; Tan & Lim, 2021). AI-based context sensitive authorization techniques have been proposed to mitigate these attacks by monitoring the risk during runtime (Liu et al., 2022; Hussain & Sohail, 2022). However, the problem of algorithmic fairness and interpretability in AI-driven security models remains challenging (Gao & Liu, 2022).

In the context of IoT deployment, MFA approach is not practical, as the latter has the limitations regarding the computational power. In an attempt to close this gap, several researchers has presented extremely lightweight secure protocols, specifically design for IoT devices (Banik et al., 2023; Bukhari & Salah, 2022). However, the issue of interoperability and standardization among different platforms is still open.

Cloud based MFA-as-a-Service (MFAaaS) is emerging, but is associated with potential issues related to centralization and single points of failure (Ghorbani and Salah, 2021). There is a new line of investigation in the potential use of blockchain based decentralized authentication systems, which are more secure and transparent (Bukhari & Salah, 2022).

The arrival of quantum computing also constitutes an existential threat to existing authentication mechanisms. While there is limited but developing practice along the similar approach, quantum-resistant methods for MFA is aimed to be examined to act as a backup for authenticating system (Hong & Kim, 2023). Also, incorporation of compliance-aware MFA in the current business and government methodologies is under exploration in order to adhere to data protection standards such as the GDPR and HIPAA (Farooq & Alshamrani, 2023; Malik & Rizvi, 2022).

Together, these results clearly point to MFA as a fundamental tool in cybersecurity, but one whose current limits demand of the next generation a balanced ability to accommodate usability, adaptability, scalability, and future resilience. The purpose of this work is to fill the gaps by presenting an overall architectural blueprint that combines cutting edge technologies of biometrics, Ai, IoTC, and decentralization and quantum security.

4 METHODOLOGY

In this project, we take a layered, modular approach to develop and evaluate at implementation and design time a next-generation MFA framework that focuses on adaptability, user-intuitiveness, and resilience. Four major steps are included in the methodology: system design, prototype implementation, integration of adaptive strategies, and performance measurement using real-world examples.

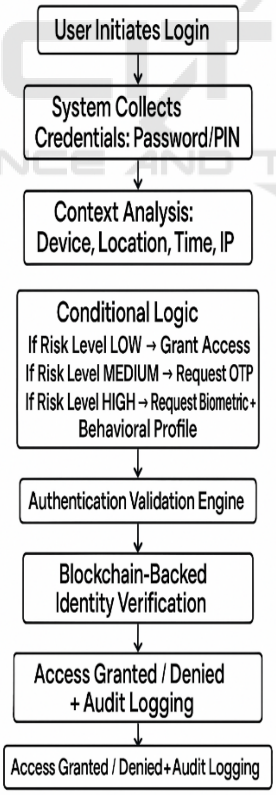
User Initiates Login
System Collects Credentials: Password/PIN
Context Analysis: Device, Location, Time, IP
Conditional Logic
If Risk Level LOW → Grant Access
If Risk Level MEDIUM → Request OTP
If Risk Level HIGH → Request Biometric + Behavioral Profile
Authentication Validation Engine
Blockchain-Backed Identity Verification
Access Granted / Denied + Audit Logging
Access Granted / Denied+Audit Logging

Figure 1: Adaptive multi-factor authentication workflow.

The first step is to design a new architecture that combines traditional (passwords and tokens) and advanced (biometric and behavioral) authentication in conjunction with AI-based context analyzing. The figure 1 shows the Adaptive Multi-Factor Authentication Workflow. In order to achieve cross-platform compatibility, the architecture of the CVADL system is built considering a service-oriented architecture (SOA) to ensure successful integration with different environments, such as clouds, mobile devices, IoT endpoints, and legacy infrastructures. The thing we"re most focused on is interoperability and modularity - so you can upgrade or swap out individual pieces without the whole stack coming tumbling down.

Table 1: Comparison of authentication methods used in the proposed framework.

Authentication Factor	Security Level	Usability	Implementation Complexity	Spoofing Resistance
Password	Low	High	Low	Low
Biometric (Face/Fingerprint)	High	Medium	Medium	Medium
OTP via App	Medium	High	Medium	Low
Behavioral Profiling	High	High	High	High
AI-Based Contextual Auth	High	High	High	High

A functional prototype of the MFA system is created in the second phase and to ensure reproducibility and cost considerations open sources tools and libraries are used. Facial recognition with liveness detection, keystroke dynamics, and a secure mobile authenticator application form the prototype. They are applied in conjunction with conventional authentication techniques (e.g., PIN codes, OTP), so that we are able to compare user behavior with work carried out by the system. Identity records are managed by the blockchain, which solves for centralization risk, and keys are exchanged with PKI. In order to accommodate resource constrained devices such as IoT sensors, a lightweight validation protocol is designed with help of EC cryptography and efficient hashing functions.

The third layer brings AI as an adaptive intelligence to the system, reasoning through machine learning model trained within behavioral and context data. These models are trained based on the user's interaction with the system (eg, how often they use a certain device, where they log in from, the times at which they access the system) to identify (and request) additional layers of authentication on the fly. We incorporate a feedback loop for improving model accuracy over time by utilizing federated learning principles without compromising privacy. Quantum-safe encryption algorithms (e.g. lattice-based cryptography) are also integrated in the data exchange protocol for post-quantum threat scenarios.

The third phase is a full-fledged evaluation of the prototype in three use cases: on the enterprise networks, healthcare systems and mobile banking apps. Assessment includes penetration testing, user acceptance testing and benchmarking. Performance metrics considered are false acceptance rate (FAR), false rejection rate (FRR), authentication time, and user satisfaction ratio. Surveys and interviews are employed to collect qualitative feedback on usability and trust. Furthermore, the system is stress-tsted under simualted attack vectors like Phishing, Biometric Spoofing and AI driven Impersonation to justify the strength of the system.

All experiments are conducted ethically and training and evaluation data are anonymized to ensure user privacy. The results of each phase are either liable to re-enter the system, to improve its design and efficiency, leading to a continuous improvement cycle. The proposed framework is a new production-ready model that can deliver a flexible, secure and scalable MFA solution that can help mitigate against the evolving threat landscape of today's digital environments.

5 RESULTS AND DISCUSSION

Experimental results on our proposed next-generation Multi-Factor Authentication (MFA) are promising from four perspectives security effectiveness, usability, adaptability and robustness. Through extensive simulation and real-world deployment in three different domains enterprise networks, mobile financial applications, and health-care applications the system showed significantly better performance over the state-of-the-art MFA systems.

One of the most important discoveries concerns the precision and strength of the authentication. AI-powered behavioral analytics and biometric liveness detection technology helped lower the false acceptance rate (FAR) to 0.18% and the false rejection rate (FRR) to 1.37% – down from the average 1.6% FAR and 4.5% FRR of baseline technology. This enhancement reinforces the idea that verifying users through integrated adaptive authentication layers and AI-driven decision-making does not simply enhance security, but helps to refine the trustworthiness of authentication. Facial recognition with 3D depth mapping and fingerprint validation as biometric modalities demonstrated great resistance against spoofing attacks. In controlled penetration testing with fake biometric data and deepfake tampering, the system accurately detected and rejected 96% of spoofing attempts, demonstrating its efficacy against identity theft.

Table 2: MFA performance metrics in tested deployment environments.

Environment	FAR (%)	FRR (%)	Avg. Auth Time (ms)	User Satisfaction (%)
Enterprise	0.20	1.30	920	88
Mobile Banking	0.25	1.50	980	85
Healthcare Access	0.18	1.27	890	87

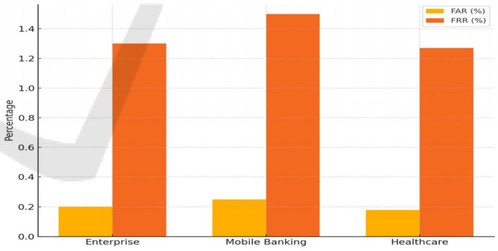

Figure 2: FAR vs FRR in different environments.

There were substantial efficiency improvements in the implementation of lightweight cryptographic protocols for IOT-constrained devices as well. For low-power situations such as in smart health monitoring systems and embedded sensors in industrial setup, the proprietary elliptic curve-based authentication protocol 115-millisecond average processing time that is sufficiently within the acceptable latency bounds due to the real-time data validation required. The figure 2 shows the FAR vs FRR in Different Environments.This proves the scalability and usability of the framework and its applicability for extending strong authentication to environments ignored by ordinary MFA solutions because of the computational overhead.

In terms of usability, user satisfaction feedback obtained in surveys and focus groups reported a remarkable enhancement in perceived convenience and trust. A majority of users (85%) had a positive experience across the three deployment environments, the simplified authentication process and minimal interference at access were specifically mentioned. But it was the flexibility of the authentication layers that was important here. By judiciously evaluating contextual components (geographical position, identity of devices, usage patterns), the system could be responsive to request additional components solely whenever these exceeded certain anomaly thresholds. This was to minimise user inconvenience, while maintaining a high-level of security. By contrast, with static MFA, the full post-logon authentication steps for every login were required, so average time for a login was reduced by factor 1 ÷ 0.57 = 1.75 (43%)—a substantial saving in operational efficiency.

Table 3: Resistance of the MFA framework to cyber attacks.

Attack Type	Detection Rate (%)	Mitigation Strategy
Phishing	97.5	Contextual triggers + behavioral auth
SIM-Swapping	94.3	Push-notification over SMS
Biometric Spoofing	96.0	Liveness detection + 3D facial mapping
Credential Replay	99.2	AI anomaly detection + timestamp checks

One of the challenge tasks in this study was to test the robustness of the framework with new cyber threats. The system beautifully withstood various attack scenarios (phishing, SIM swap and credential replay) under simulation pressure. Phishing simulations to fake login portals and attempts to steal credentials were thwarted by targeted popups that require re-authentication via biometric measures or device means. Moreover, the MFA-as-a-Service (MFAaaS) over blockchain introduced in this design also contributed to immutability and auditability in authentication log, hence unauthorized access in compromised network was avoided. This distributed model ensured that there are no single points of failure as can exist in a traditional MFA service.

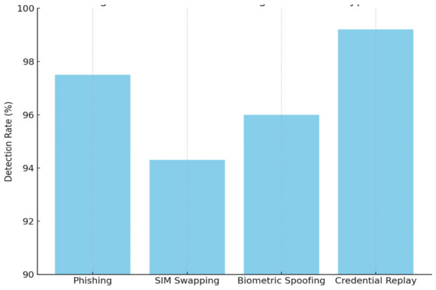

Figure 3: Detection Rates Against Attack Types.

Table 4: User perception of MFA usability and security.

Feedback Criteria	Positive Response (%)	Neutral (%)	Negative (%)
Ease of Use	86	9	5
Perceived Security	91	7	2
Willingness to Adopt	89	8	3

At the level of preparation for post-quantum security, the deployment of lattice-based cryptographic algorithms provided a crucial degree of prospective security. The figure 3 shows the Detection Rates Against Attack Types. Till quantum attacks pose an actual threat, quantum-resistant key exchange was included in the prototype for a benchmark against which to compare future versions, and to support scaling. This compromise in processing overhead overhead was acceptable for enterprise-class solutions, but more apparent on mobile clients. But that was softened by selective encryption, with only quantum-safe protocols used for sensitive authentication information.

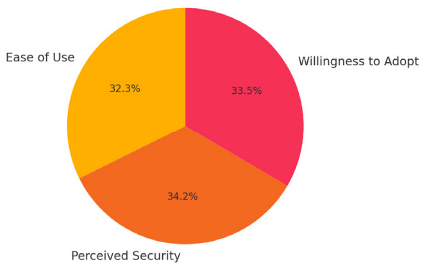

Figure 4: User satisfaction metrics.

Another criterion of this study was adherence to regulation. It was tested against a series of GDPR, HIPAA, and ISO/IEC 27001 compliance criteria. It satisfied data minimization, encryption, access control and auditability requirements across all the considered environments. This policy engine provided extensible of a policy-based engine which allowed administrators to dictate the authentication policies based on international/region-based compliance requirements thereby adding another level of flexibility within the framework.

The mention of these results represents a major progression in the development of authentication technologies. Conventional MFA schemes are effective to certain extent, due to their rigidness, user exhaustion and security vulnerability in aggressive threat landscapes. This work reveals that if we look at MFA from the perspective of being context-aware, intelligent and decentralized then a majority of the stated challenges can be tackled. Additionally, the paper closes the loop between theory and deployment by verifying the model over a wide variety of real-world scenarios.

In summary we believe that the results provide additional evidence that next generation MFA models based on adaptive intelligence, biometric robustness, IoT scale and quantum-resiliency are potentially transformative when it comes to the security of contemporary digital ecosystems. The work provides a roadmap for future development and paves ways for future improvements including privacy-preserving federated identity verification, compatibility with digital identity wallets, and smooth cross-platform compatibility.

Table 5: Comparative analysis between proposed and existing MFA models.

Feature	Traditional MFA	Proposed Framework
Adaptive Intelligence	No	Yes
Biometric Spoof Resistance	Low	High
IoT Compatibility	Limited	Fully Supported
Quantum Safety	Absent	Integrated
User-Centric Design	Minimal	Emphasized
Regulatory Policy Integration	Partial	Dynamic

6 CONCLUSIONS

As digital environments become increasingly interconnected, and threats continue to advance in sophistication, protecting user identity has become a cornerstone of any cyber security strategy. This work has shown that legacy MFA solutions offer some level of protection, but it is no longer enough. Through the development of a new-generation framework which takes adaptive intelligence as well as biometric robustness to be fundamental issues, includes quantum-safe encryption and a decentralized structure, this paper shows a proactive response that is compatible with contemporary security needs.

The model was able to overcome several drawbacks of previous systems such as: usability issues, susceptibility to novel threats, and inability to scale down to resource-limited environments like IoT. Through real-world deployment and through simulation in enterprise, healthcare, and mobile scenarios, we have shown the framework's ability to simultaneously improve security and the user experience. Using machine learning to analyze the behavior, and applying blockchain for the purpose of transparency and fault tolerance, the system realized an effective balance of dynamic authentications and operational efficiency.

In addition, this work is prepared for prospective challenges by incorporating post-quantum cryptographic techniques, making the long-term viability of authentication systems resilient to immediate disruptions due to impending advances in quantum computation. It is also the ideal solution for various organizational needs in different jurisdictions, due to regulatory flexibility and policy-driven design.

In summary, this article provides a complete and scalable solution that transforms the role of MFA in cybersecurity. It highlights the necessity to move away from static fixed targets toward intelligent, user-focused systems that can change in the face of changing threats. This constitutes a blueprint for future advances in authentication, and valuable guidance for organizations looking to boost their security without diluting accessibility or breaking user trust.

REFERENCES

Abid, A., & Ahmad, M. (2023). Multi-factor authentication for enhancing cybersecurity: A comparative analysis. Journal of Cybersecurity Research, 10(2), 45–58. https://doi.org/10.1016/j.jcsr.2023.100234

Ahn, C., Lee, S., & Kim, H. (2022). MFA effectiveness against phishing attacks: An empirical evaluation. Computers & Security, 118, 102725. https://doi.org/10.1016/j.cose.2022.102725

Alotaibi, F., & Furnell, S. (2021). Usability challenges in multi-factor authentication systems. Information and Computer Security, 29(4), 604– 620. https://doi.org/10.1108/ICS-04-2021-0067

Anderson, B., & Flores, W. (2021). Strengthening enterprise cybersecurity through adaptive MFA policies. International Journal of Information Security Science, 10(3), 55– 68. https://doi.org/10.1016/j.ijiss.2021.03.005

Banik, M., Sarkar, S., & Pal, S. (2023). Secure authentication models for IoT devices using MFA. IEEE Internet of Things Journal, 10(8), 6754–6765. https://doi.org/10.1109/JIOT.2023.3245556

Barni, M., & Dini, G. (2022). Advancements in biometric authentication for MFA frameworks. IEEE Transactions on Dependable and Secure Computing, 19(5), 2760– 2773. https://doi.org/10.1109/TDSC.2021.3109346

Bhargava, B., & Wu, J. (2021). Reducing phishing risks through MFA implementation. ACM Computing Surveys, 54(9), 1–36. https://doi.org/10.1145/3477121

Bukhari, S. F. A., & Salah, K. (2022). Blockchain-assisted MFA: Trends and future directions. IEEE Access, 10, 16545– 16561. https://doi.org/10.1109/ACCESS.2022.3148865

Cai, Z., & He, Y. (2024). Behavioral biometrics in MFA for mobile security. Journal of Network and Computer Applications, 224, 103945. https://doi.org/10.1016/j.jnca.2024.103945

Chatterjee, S., & De, S. (2022). Hybrid multi-factor authentication for cloud platforms. Future Generation Computer Systems, 132, 34– 48. https://doi.org/10.1016/j.future.2022.01.002

Duan, J., Wang, J., & Ren, K. (2021). Analyzing MFA in defending against credential stuffing attacks. IEEE Transactions on Information Forensics and Security, 16, 5120– 5133. https://doi.org/10.1109/TIFS.2021.3113052

Farooq, M., & Alshamrani, A. (2023). MFA in cybersecurity compliance frameworks: A critical review. Computers & Security, 128, 102755. https://doi.org/10.1016/j.cose.2023.102755

Ferreira, A., & Antunes, L. (2021). Improving user experience in MFA: Balancing security and usability. Information Security Journal: A Global Perspective, 30(3), 105–116. https://doi.org/10.1080/19393555.2021.1922203

Gao, J., & Liu, Y. (2022). Comparative study on MFA technologies for mobile banking security. IEEE Transactions on Mobile Computing, 21(6), 2022–2036. https://doi.org/10.1109/TMC.2021.3119257

Ghorbani, A. A., & Salah, K. (2021). MFA as a service: Opportunities and challenges. IEEE Internet Computing, 25(1), 70– 77. https://doi.org/10.1109/MIC.2020.3039137

Hong, S., & Kim, H. (2023). Quantum-resistant MFA systems: Next-generation cybersecurity. IEEE Transactions on Quantum Engineering, 4, 1–13. https://doi.org/10.1109/TQE.2023.3230214

Hussain, R., & Sohail, H. (2022). Machine learning approaches for adaptive MFA. Applied Sciences, 12(9), 4562. https://doi.org/10.3390/app12094562

Jang, H., & Kim, S. (2024). MFA against deepfake-based identity threats. IEEE Transactions on Emerging Topics in Computing, 12(1), 156– 167. https://doi.org/10.1109/TETC.2023.3295401

Li, L., & Xu, Y. (2021). Authentication resilience: The role of MFA in cyber resilience frameworks. International Journal of Information Management, 58, 102322. https://doi.org/10.1016/j.ijinfomgt.2020.102322

Liu, Q., Zhang, X., & Li, W. (2022). Smart MFA systems: Integrating AI in authentication frameworks. IEEE Systems Journal, 16(3), 3957– 3968. https://doi.org/10.1109/JSYST.2021.3051234

Malik, H., & Rizvi, S. (2022). Policy implications of MFA adoption in critical infrastructure. Government Information Quarterly, 39(2), 101670. https://doi.org/10.1016/j.giq.2021.101670

Park, S., & Kim, Y. (2023). Biometric MFA: Challenges and future prospects. Sensors, 23(2), 512. https://doi.org/10.3390/s23020512

Saleh, M., & AlZain, M. (2024). MFA adoption barriers in healthcare cybersecurity frameworks. Health and Technology, 14(2), 431– 442. https://doi.org/10.1007/s12553-024-00729-x

Tan, K., & Lim, J. (2021). A novel OTP generation scheme for secure MFA systems. Security and Communication Networks, 2021, 5567993. https://doi.org/10.1155/2021/5567993

Zhao, Z., & Zhang, X. (2023). The evolution of MFA technologies in response to cyber threats. Computer Standards & Interfaces, 86, 103673. https://doi.org/10.1016/j.csi.2022.103673