International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 01 | Jan 2026 www.irjet.net p-ISSN: 2395-0072

Multi-Factor Authentication

Yash Vinod Tayade[1], Mrs. Neha N. Jamdar[2], Dr. Emmanuel Markappa[3]

[1]*Dept. of Information Technology, Pune Institute of Computer Technology, Pune, Maharashtra, India*
[2]*Professor, Dept. of Information Technology, Pune Institute of Computer Technology, Pune, Maharashtra, India*
[3]*Professor, Dept. of Information Technology, Pune Institute of Computer Technology, Pune, Maharashtra, India*

---***---

Abstract - *Authentication is the main gatekeeper in the modern digital environment, preventing access to information systems by unauthorized users. Password-only authentication is susceptible to phishing, brute-force attacks, and credential leaks, which is why the Multi-Factor Authentication (MFA) has come to the rescue. MFA makes authentication more secure by using two or more different factors that include knowledge (password), possession (token or mobile device), and inherence (biometrics). Still, traditional MFA solutions face difficulties with their user interface, dependent factors, and doubtful security in the real world despite being generally used. The manuscript details the review of MFA progression, summarizing the central points from four major research papers of Ometov et al. (2018), Li et al. (2021), Wang and Wang (2023), and Paredes-García et al. (2025), correspondingly. The paper highlights the innovation in the Threshold Multi-Factor Authentication (T-MFA), Self-Sovereign Identity (SSI), Zero Knowledge Proofs (ZKP), and Shamir's Secret Sharing (SSS) fields. Besides, it deals with the eight failure categories in formal security proof of MFA, thus, bridging the significant theoretical practical security gap. Research shows that future MFA systems are to be flexible, decentralized and cryptographically verifiable with features of privacy and resilience in different real-world scenarios like finance, IoT, healthcare, and cloud infrastructure.*

***Key Words*: Multi-Factor Authentication, Threshold MFA, Cryptography, Zero-Knowledge Proof, Secret Sharing, Provable Security, Self-Sovereign Identity, Blockchain, Privacy-Preserving Authentication.**

1. INTRODUCTION

In a hypersensitive world where the digital identity of a person is becoming more and more valuable, the need to secure the access to online systems is the first requirement. Single-Factor Authentication (SFA)—the traditional password mechanism—has been mostly kept as a method because of its simplicity but presents some serious risks. The major problems connected with a single-factor authentication system are password reuse, weak combinations, phishing attacks, and large-scale credential leaks that all have demonstrated that using only one factor is not enough to protect modern systems.

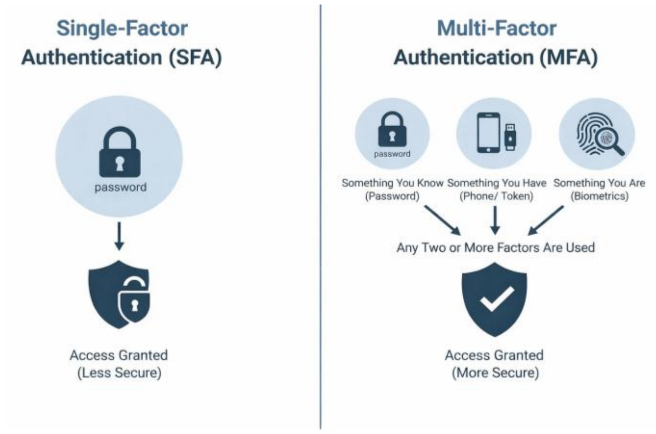

Fig -1: Comparison of Single-Factor and Multi-Factor Authentication.

Multi-Factor Authentication (MFA) was introduced as a solution of layered defenses which implied that users must authenticate via multiple independent factors:

- One that you know – passwords, PINs, or answers to security questions.
- One that you have – smart cards, hardware tokens, or mobile devices.
- One that you are – biometric or behavioral identifiers such as fingerprints, facial patterns, or voice recognition.

Thus MFA prevents unauthorized access by several factors (one of which is presumably compromised) from happening. However, several practical limitations have been revealed due to its extensive deployment:

- Rigidity: Traditional MFA necessitates certain combinations (e.g., password + OTP). Users are unable to access their accounts if one factor is missing.
- Problems of usability: Users experience inconvenience with multiple verification steps and therefore, refuse to use MFA further.
- Security assumptions: Although some "formal proofs" are claimed by many systems, they ignore the impact of the device theft or malware on the security of the system.

The recent works on threshold cryptography, decentralized identity, and privacy-preserving cryptographic proofs are motivated by a desire to solve the abovementioned problems. Threshold MFA based on the idea of any t out of n registered factors allows authentication whereas self-sovereign identity (SSI) changes the model of identity management to ensure user control. This paper reviews these innovations and reflects on their possible implementation in the forthcoming digital ecosystems.

2. LITERATURE REVIEW

2.1 Classical MFA and Its Evolution

Ometov et al. (2018) conducted one of the earliest comprehensive reviews of MFA, charting its evolution from SFA to Two-Factor (2FA) and ultimately to modern Multi Factor Authentication. Their survey categorized authentication methods into three distinct groups—knowledge, possession, and biometric factors—illustrating how the combination of these factors increases system security. They further evaluated MFA performance using parameters such as False Accept Rate (FAR) and False Reject Rate (FRR), which quantify the trade-off between usability and security. Om etov's analysis also emphasized that while biometric integration improved security, it raised new privacy challenges, especially when biometric templates are stored on centralized servers. The key insight from this study is that MFA's true strength lies not just in adding more factors but in how effectively these factors are integrated, managed, and verified without compromising user experience.

2.2 Threshold Multi-Factor Authentication (T-MFA)

Li et al. (2021) introduced a groundbreaking concept called Threshold Multi-Factor Authentication (T-MFA) which made a significant departure from traditional MFA. Normally, MFA involves a fixed set of factors, but with T-MFA, a user is allowed to verify their identity with any t out of n registered factors. For example, if a single user has five different authentication factors like a password, smartphone, smartwatch, biometric ID, and home PC, then this user can authenticate with any three (t=3) of these, depending on which are available.

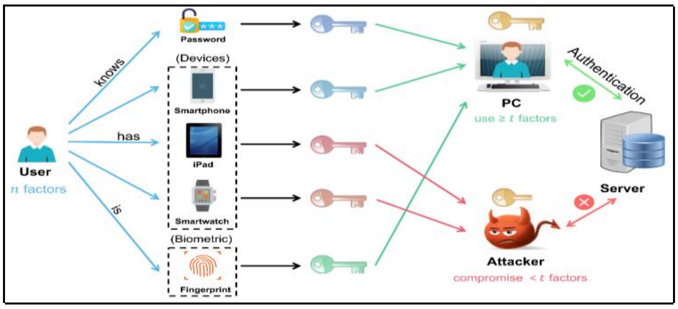

Fig -2: Threshold-based MFA allowing any t of n authentication factors.

The T-MFA Key Exchange (T-MFAKE) protocol that they designed locally combines threshold cryptography with an Oblivious Pseudorandom Function (TOPRF) to create session keys without disclosing the factors used. In this arrangement, the notion of factor invisibility is introduced, thus, even if the server is cracked, it cannot infer which authentication factors are being used. Additionally, through the use of fuzzy extractors, the protocol changes biometric data into cryptographic keys while still keeping the data private—thus not allowing the biometric data to be reconstructed even if the storage is compromised. The protocol is efficient enough to complete only two communication rounds which is proof of its effectiveness in real-world scenarios. T-MFA is an excellent example of how security, user convenience, and fault tolerance can be harmonized thus; it has solved the issue that was the greatest drawback of conventional MFA systems.

2.3 Failures in Security Proofs of MFA

Many MFA systems claim to be "formally proven secure," yet they often fail when exposed to real-world threats. In their 2023 study, Wang and Wang analyzed 70 MFA protocols and uncovered eight main reasons behind these failures, such as:

1. Incomplete modeling of adversaries
2. Unrealistic or oversimplified threat assumptions
3. Misuse of cryptographic techniques
4. Ignoring how authentication factors interact
5. Flawed use of the random oracle model
6. Poor defense against side-channel attacks
7. Lack of forward secrecy
8. Weak or incorrect reduction proofs

Their research showed that while many systems appear strong on paper, they often overlook practical issues like stolen smart cards, compromised devices, or phishing-based breaches. By identifying and classifying these weaknesses, Wang and Wang created a framework to better evaluate MFA systems in a more realistic way.

Overall, their work highlights the need to balance theoretical security with practical testing—ensuring that MFA solutions are not only mathematically sound but also resilient in the real world.

2.4 Self-Sovereign Identity (SSI) and MFA

Paredes-García et al. (2025) introduced SIBERIA, a framework that combines Self-Sovereign Identity (SSI) with Multi-Factor Authentication (MFA) to give users full control over their digital identities. Instead of depending on centralized identity providers, SIBERIA uses decentralized identifiers (DIDs) and verifiable credentials (VCs) managed through blockchain technology. This ensures that users own and manage their identity data directly while keeping it secure and private. The framework supports advanced biometric factors such as voice recognition and behavioral patterns, aligning with global data protection standards like GDPR and eIDAS 2.0. By decentralizing identity management, SSI reduces the chances of mass data breaches and builds a more trustworthy authentication process.

Each identity verification in SIBERIA is recorded on the blockchain through smart contracts, ensuring transparency, auditability, and privacy. When combined with MFA, SSI creates a trustless authentication system, meaning that no single authority controls the process—security is guaranteed by the technology itself

Overall, SIBERIA shows how decentralized identity systems can enhance security in sensitive sectors like industrial operations and healthcare, where continuous and reliable authentication is essential.

3. METHODOLOGY / SYSTEM ARCHITECTURE

Modern Multi-Factor Authentication (MFA) systems rely on advanced cryptographic techniques and decentralized architectures to balance security, privacy, and flexibility. Three key technologies—Threshold Cryptography, Zero Knowledge Proofs (ZKP), and Self-Sovereign Identity (SSI)—are shaping the next generation of authentication systems.

3.1 Threshold Cryptography and Secret Sharing

Threshold cryptography enhances security by dividing a secret key into multiple parts (called shares). Only a specific number of shares (t out of n) are needed to reconstruct the secret. This idea is based on Shamir's Secret Sharing (SSS), where:

$$K = f(0)$$

Here, f(x) is a polynomial of degree (t−1), and any t valid points can recover the original key K.

In MFA, each authentication factor—such as a device, biometric, or token—holds one share of the secret. Access is granted only when the required numbers of valid factors are presented. This method provides two major benefits:

- Fault tolerance: Users can still authenticate even if one factor (like a device) is unavailable.
- Resistance to compromise: An attacker cannot reconstruct the secret without collecting enough valid shares.

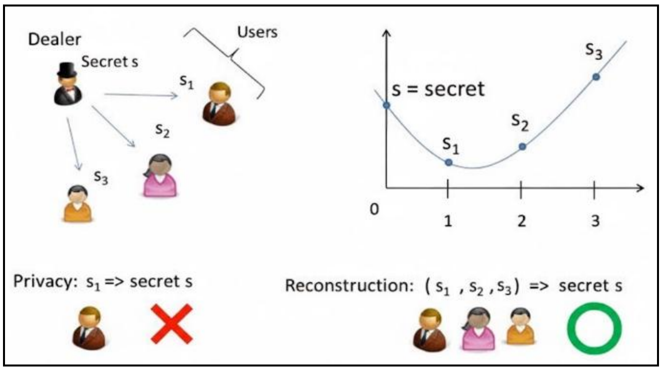

Fig -3: Secret sharing approach used in threshold-based MFA.

3.2 Zero-Knowledge Proofs (ZKP)

Zero-Knowledge Proofs allow one party to prove that they know a secret without revealing the secret itself. In MFA, this technique lets trusted devices or users verify their identity without exposing internal credentials or identifiers. For example, a smartphone could prove it's authorized without sending its hardware ID or cryptographic key to the server. This greatly reduces the risk of data leaks and supports compliance with privacy laws such as GDPR.

ZKPs can also strengthen threshold cryptographic systems by verifying that each share is valid—without disclosing any sensitive information—adding an extra layer of trust and transparency.

3.3 Self-Sovereign Identity (SSI) Integration

When MFA is combined with Self-Sovereign Identity (SSI), identity management becomes fully decentralized. Instead of relying on centralized databases, users keep their digital identities in personal wallets, which store verifiable credentials (like certificates or licenses). These credentials can be independently validated through cryptographic proofs and blockchain records.

SSI ensures:

- User control: Individuals decide what data to share and with whom.
- Cross-platform use: The same credentials can be used securely across multiple systems.
- Tamper-evidence: Block chain ensures that identity records cannot be altered without detection.

This combination of SSI and MFA enables privacy preserving, decentralized authentication ecosystems.

4. DISCUSSION AND COMPARATIVE ANALYSIS

Table -1: Comparative Analysis of Multi-Factor Authentication Research

Authors	Year	Key Contribution	Core Strength	Security Approach / Methodology	Evaluation / Findings	Limitation
Ometov et al.	2018	Defined MFA evolution and classified authentication factors into knowledge, possession, and biometrics. Introduced comparative metrics like FAR and FRR for usability–security trade-off.	Comprehensive survey establishing foundational understanding of MFA.	Analytical literature review; factor classification; risk-based discussion.	Demonstrated that usability and privacy remain critical trade-offs even in multi-layer authentication.	Lacks formal cryptographic modeling and quantitative comparison; focuses mainly on conceptual discussion.
Li et al.	2021	Proposed **Threshold Multi-Factor Authentication (T-MFA)** and designed **T-MFAKE protocol** integrating threshold cryptography and Oblivious PRF.	Highly flexible and efficient; supports authentication with any *t* of *n* factors; resistant to server compromise.	Cryptographic design; theoretical proofs of security; simulation-based performance analysis.	Achieved two-round communication efficiency; demonstrated resistance to replay and factor compromise attacks.	Deployment complexity; computational cost grows with number of registered factors; limited real-world validation.
Wang & Wang	2023	Identified **eight categories of failures** in security proofs of MFA systems; created framework for analyzing proof soundness.	Offers a diagnostic foundation for evaluating theoretical security claims; bridges theory and practice.	Systematic taxonomy and proof-based analysis; adversarial model comparison.	Highlighted that many "provably secure" MFA schemes fail in real-world conditions; emphasized stronger adversary modeling.	Lacks experimental or prototype testing; focuses on theoretical vulnerability assessment.
Paredes-García et al.	2025	Developed **SIBERIA**, a Self-Sovereign Identity (SSI)-based MFA framework combining verifiable credentials, decentralized identifiers, and	Fully decentralized, privacy-preserving architecture compliant with GDPR and eIDAS 2.0.	System implementation and case-study validation in industrial environments.	Achieved trustless authentication and continuous verification; strong identity privacy and interoperability.	High computational and storage overhead; latency concerns in blockchain verification; limited scalability on low-power devices.

		blockchain.				
Proposed Integration Insight (Survey Conclusion)	—	Synthesis of all approaches — combining **Threshold MFA** flexibility, **SSI** decentralization, and **ZKP** privacy protection.	Provides a unified direction for next-generation MFA systems.	Hybrid cryptographic–decentralized design integrating T-MFA, SSI, and ZKP concepts.	Promises adaptive, privacy-preserving, and verifiable authentication for real-world sectors (finance, IoT, healthcare).	Still theoretical; requires efficient, lightweight cryptography and cross-domain standardization for scalability.

5. APPLICATIONS AND FUTURE WORK

5.1 Applications

Multi-Factor Authentication (MFA) is finding use across a wide range of industries, each leveraging its strengths for enhanced security and trust.

1. Banking and E-Payments: MFA protects users from account hijacking by combining device-based verification, biometrics, and transaction-level authentication to prevent fraud.
2. Cloud Services: It ensures secure access to sensitive data by pairing traditional passwords with hardware security keys or behavioral patterns, reducing risks from stolen credentials.
3. Healthcare: Patient data is safeguarded using SSI based verifiable credentials and decentralized access logs, ensuring privacy and compliance with data protection laws.
4. IoT Devices: Threshold MFA spreads authentication trust across multiple devices, removing the danger of a single-point failure in connected environments.
5. E-Governance: Governments can use blockchain backed decentralized IDs to enable secure, transparent, and citizen-controlled authentication for online services.

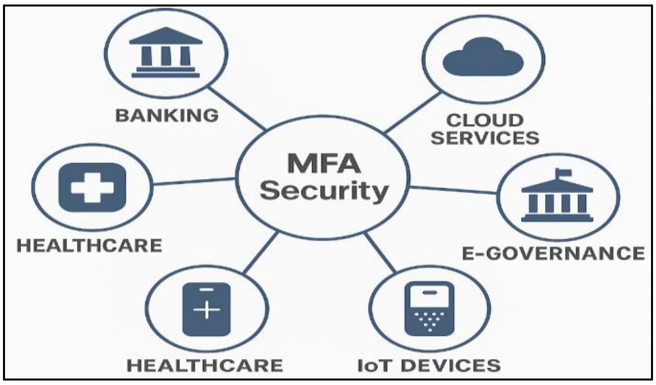

Fig -5: Major application areas of Multi-Factor Authentication.

5.2 Future Research Directions

As digital ecosystems evolve, MFA must adapt to new challenges. Future research is focusing on:

1. AI-Driven MFA: Building adaptive systems that analyze user behavior and context to automatically adjust authentication levels based on risk.
2. Lightweight Cryptography: Creating efficient cryptographic algorithms designed for low-power IoT devices without compromising security.
3. Post-Quantum Security: Developing MFA methods that remain secure even against attacks from future quantum computers.
4. Cross-Domain Interoperability: Establishing global standards to integrate SSI, blockchain, and MFA technologies, ensuring smooth and consistent authentication across platforms.

Together, these advancements aim to make MFA not only stronger but also smarter, more user-friendly, and better suited for a decentralized digital future.

6. CONCLUSION

Multi-Factor Authentication has become a key part of modern cybersecurity that has gone through a significant change to highly secure frameworks from static password systems. Innovations like Threshold MFA, Zero-Knowledge Proofs, and Self-Sovereign Identity have opened the door to more intuitive and privacy-respecting MFA solutions. Nevertheless, efforts to make them scalable, acceptable to users, and efficient in terms of cryptographic operations are still ongoing. The future of authentication depends on the creation of adaptive, decentralized, and verifiable identity verification methods that can guarantee users' security and offer them convenience. MFA, supported by both cryptographic theory and practical resilience, has the potential to become the core of secure identity management in the digital world.

REFERENCES

[1] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” Cryptography, vol. 2, no. 1, pp. 1–31, 2018.

[2] W. Li, H. Cheng, P. Wang, and K. Liang, “Practical Threshold Multi-Factor Authentication,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3573–3588, 2021.

[3] Q. Wang and D. Wang, “Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices,” IEEE Transactions on Information Forensics and Security, vol. 18, pp. 597–612, 2023.

[4] D. Paredes-García et al., “SIBERIA: A Self-Sovereign Identity and Multi-Factor Authentication Framework for Industrial Access,” Applied Sciences, vol. 15, no. 8589, pp. 1–36, 2025.