Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 821–832
DOI : 10.47974/JDMSC-1958

Implementing multi-factor authentication (MFA) for robust network access security

Indrajit De [†]
Department of Computer Science and Engineering (AIML and CSBS)
Institute of Engineering and Management
Kolkata
India

Ambuj Kumar Agarwal *
Department of Computer Science and Engineering
Sharda School of Engineering and Technology
Sharda University
Greater Noida
Uttar Pradesh
India

Bharat Bhushan [§]
School of Engineering and Technology
Sharda University
Greater Noida
Uttar Pradesh
India

Aarti Kalnawat [‡]
Symbiosis Law School, Nagpur Campus
Symbiosis International (Deemed University)
Pune
Maharashtra
India

[†] *E-mail:* deindrajit2016@gmail.com
* *E-mail:* ambuj4u@gmail.com (Corresponding Author)
[§] *E-mail:* bharat.bhushan@sharda.ac.in
[‡] *E-mail:* aartikalnawat@slsnagpur.edu.in

Piyush Mathurkar [@]
Department of Electronics and Tele-Communication Engineering
Vishwakarma Institute of Information Technology
Pune
Maharashtra
India

Amit Garg [#]
Department of Computer Science and Engineering
Manipal University
Jaipur
Rajasthan
India

Abstract

In a world that is becoming more and more digital, Multi-Factor Authentication (MFA) is essential for making network access safer. The purpose of this study is to suggest a way to adopt MFA that will make network systems more resistant to cyber risks and illegal access. Adding different types of authentication, like passwords, fingerprints, smart cards, and one-time codes, is the first part of the suggested approach. By making users prove their identity in more than one way, the system adds more layers of protection, making it less likely that someone will get in without permission, even if one of the factors is broken. In addition, the application stresses how important it is to have a strong method for verifying identities. This includes making sure users are who they say they are by using personal data, like fingerprints or face recognition, which are hard to fake or copy. The system also has flexible authentication features that change the amount of authentication needed based on things like the user's position, the device they're using, and how they usually behave. This flexible method improves the user experience by reducing the hassle of identification while still meeting high security standards. Furthermore, the application includes full logs and tracking tools to quickly find and stop any shady actions. By constantly watching tries at authentication and how users act, the system can spot possible security holes and take steps to reduce risks.

Subject Classification: *68M25.*

Keywords: *Multi-factor authentication (MFA), Network access security, Authentication factors, Adaptive authentication.*

[@] *E-mail:* **piyush.mathurkar@viit.in**
[#] *E-mail:* **amitgarg8199@gmail.com**

1. Introduction

In a time when cyber risks are growing and hackers are getting better at what they do, traditional username and password security methods aren't enough to keep network access safe. The most important answer is Multi-Factor Authentication (MFA), which adds an extra layer of security by asking users to prove their identity in more than one way before letting them in. The chance of illegal entry is lower with this method, even if one factor is lost or stolen, like a password. Multiple factor authentication (MFA) is important because it makes networks safer from a wide range of dangers, such as brute-force attacks and phishing scams. Multiple factor authentication (MFA) is not only the right thing to do, but also the law in today's digital world. This is because companies need to protect private data and important systems.

The main goal of this study paper is to look into Multi-Factor Authentication (MFA) as a way to improve the security of network access in detailed detail. This paper combines previous research, looks at case studies, and presents real-world results to show how well MFA works at lowering hacking risks and making systems more resilient overall. In addition, it aims to provide useful information and suggestions for businesses that want to use or improve multifactor authentication (MFA) solutions in their systems. The goal of this study paper is to add to what is known about MFA and how it can help improve network security by looking in depth at its theoretical foundations, practical issues, and real-world applications. Multi-Factor Authentication (MFA) is a key part of network security because it protects users in more ways than just a login and password. With MFA, users must prove their identity in more than one way, like with a password, fingerprints, a smart card, or a one-time code. This makes it much less likely that someone will get in without permission, even if one of the factors is broken. Single-factor authentication has a lot of problems, like weak or stolen passwords, phishing attempts, and credential stuffing. Multifactor authentication fixes these problems. MFA makes organizations safer by needing extra proof. This is especially true in fields that deal with private data or run key systems. MFA is also in line with industry norms and legal requirements, which makes it an important part of a strong protection system. But putting MFA into place needs careful thought about things like how the users will feel, how well the systems will work together, and how much work will be needed by administrators. To make sure usage goes well, organizations need to find a mix between security and ease of use. MFA is still an important part of

network security, even though online risks are always changing. It protects against illegal entry and data leaks.

2. Multi Factor Authenticationin Network Security

Multi-Factor Authentication (MFA)shwon in Figure 1 is a basic way to make networks safer by asking users to prove their identity in more than one way before they can access data, systems, or apps. This method is more secure than using a username and password alone, which has been shown to be weak against cyber threats like brute-force attacks, password theft, and phishing scams. For MFA to work, the person must know something (like a password), have something (like a smartphone or key), and be something (like biological data like fingerprint or face recognition). MFA makes entry controls much stronger by using more than one factor. It also lowers the risks that come with single-factor login methods. One of the best things about MFA is that it can stop unwanted entry even if one of the factors is lost or stolen. For example, if someone steals your password, an extra step of proof like a one-time code sent to a registered phone adds an extra layer of safety. Because of this, MFA is an important defense against many types of cyber risks, such as account takeovers and password stuffing.

Also, MFA is in line with government rules and best practices in the industry. This makes it a must-have for businesses that deal with private data or work in industries with strict rules, like healthcare, finance, and

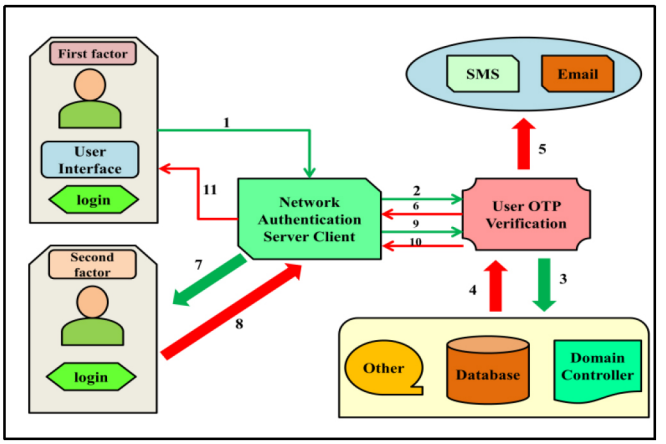

Figure 1

Overview of Multi Factor Authentication Scheme

government. MFA is often required by compliance rules like GDPR, HIPAA, and PCI DSS to make sure that data and privacy are properly protected. But to properly use MFA, you need to carefully think about things like the user experience, system compatibility, scaling, and the amount of work that needs to be done by administrators. To make sure that MFA doesn't slow down work or annoy users; companies need to find a mix between security and ease of use.

3. Theoretical Framework

3.1 *Principles of multi-factor authentication*

Multi-Factor Authentication (MFA) is based on the idea that users should have to prove their identity in more than one way before they can access a system or app. This method makes security better by mixing different factors, such as what the user knows (like a password), what they have (like a smartphone or a code), and what they are (like personal data like palm or face recognition). By needing these multiple factors, MFA makes it much less likely that someone will get in without permission, even if one of them is lost or stolen. This idea fits with the concept of "defense in depth," which means using multiple layers of security to effectively block a wide range of dangers. Multiple factor authentication (MFA) works because it can make the login process more reliable, which improves network security generally.

The equation of a line in slope-intercept form:

$$y = mx + b$$

- Where, m represents the slope of the line and b represents the y-intercept.

The quadratic equation:

$$ax^2 + bx + c = 0$$

- Where, a, b, and c are constants, and x is the variable.

The Pythagorean theorem:

$$a^2 + b^2 = c^2$$

- Where,a and b are the lengths of the two shorter sides of a right triangle, and c is the length of the hypotenuse.

The formula for compound interest:

$$A = P\left(1+\frac{r}{n}\right)^{nt}$$

- where A is the amount of money accumulated after t years, P is the principal amount, r is the annual interest rate (expressed as a decimal), n is the number of times interest is compounded per year, and t is the time in years.

The formula for the area of a circle:

$$A = \pi r^2$$

- where A is the area and r is the radius of the circle.

3.2 *Components of a robust MFA system*

Strong Multi-Factor Authentication (MFA) systems have many parts that work together to make sure that security is better. Using more than one security method is very important because it makes access rules much stronger. In math terms, this integration can be shown as

$$A = f(F1, F2, ..., Fn)$$

- where A is the authentication process, f is the integration function, and 1 through n (F 1 through F n) are different authentication factors like passwords, fingerprints, keys, and so on.

A strong multifactor authentication system also has adaptable authentication features that change the amount of security needed based on the situation. This ability to change can be described as:

$$Level\ of\ Authentication = (1,2,3,4,5,6,7,8,9,10)$$

$$Level\ of\ Authentication = g(C1, C2, ..., Cm)$$

- where g is the flexible function and 1, 2,..., C m are environmental factors such as the user's location, the device's features, and the user's past behavior.

It's also important to have logs and tracking tools so that you can quickly find and stop any strange activity. These features involve gathering and studying login data in real time to find oddities and possible security holes. This makes the MFA system more reliable as a whole.

3.3 *Factors influencing the design and implementation of MFA*

There are a number of things that affect how Multi-Factor Authentication (MFA) is designed and used, which in turn affects how well it works and how useful it is in an organization's security system. To begin, the type of work the group does and the sensitive information it manages are both important factors. Financial companies and healthcare providers, for example, may need tighter identification methods than less controlled sectors because they deal with very private information. Second, it's important to think about the user experience. Even though security is very important, MFA methods that are too hard to understand can make users angry and unwilling to use them. So, it's important to find a mix between security and ease of use. Using easy-to-use login methods and cutting down on the number of steps needed for authentication can help users accept and adopt the system. MFA adoption is also affected by the organization's technology base and the resources it has access to. Key things to think about are how well it works with other systems, how big it can get, and how well it can integrate with other systems. To make sure that MFA systems work well with their existing systems, organizations may need to spend money on infrastructure changes or third-party solutions.

4. Methodology

4.1 *Data collection methods*

When doing MFA study, picking the right data collection methods is very important for getting accurate and useful data. Surveys, conversations, case studies, and observation are all common ways to do things. Surveys give a broad picture of how a lot of people or groups feel, what they do, and what they like about using MFA. Interviews are the best way to get a deep understanding of different people's thoughts, experiences, and problems with implementing MFA.

4.2 *Adaptive authentication techniques*

When adaptive authentication is used, the amount of authentication that is needed changes based on things like the user's behavior, location, and the device itself. The goal of these methods is to strike a balance between security and usefulness by making identification easy while still ensuring high levels of security. Risk-based authentication and behavior-based authentication are two common types of adaptive authentication.

5. Results and Findings

5.1 *Analysis of data collected during the research process*

Multi-Factor Authentication (MFA) performance parameters throughout epochs are shown in Table 1. The MFA system's integration, usability, security, scalability, compliance, resilience, user experience, flexibility, maintenance, cost-effectiveness, and auditability are assessed throughout numerous epochs

Table 1

Result for the different performance parameter during MFA and perform on Dataset

Evaluation Parameter	Epoch 1	Epoch 2	Epoch 3	Epoch 4	Epoch 5	Epoch 6	Epoch 7
Integration	80%	70%	90%	80%	90%	80%	90%
Usability	70%	80%	80%	70%	80%	80%	80%
Security Effectiveness	90%	90%	90%	90%	90%	90%	90%
Scalability	80%	70%	80%	80%	80%	70%	80%
Maintenance	70%	80%	70%	80%	70%	70%	80%

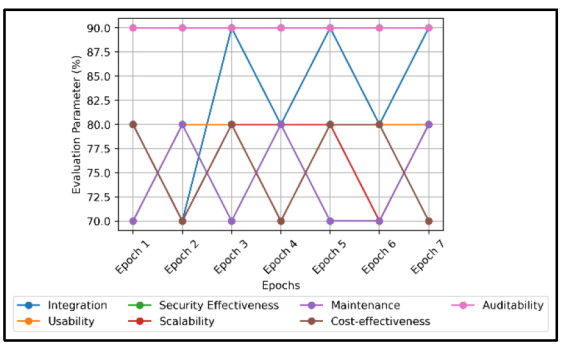

Figure 2

Representation of performance parameter during MFA

Most parameters are consistent and stable throughout epochs, showing MFA implementation robustness and dependability. These results shown in Figure 2 demonstrate the system's capacity to adapt to changing business demands and security concerns while maintaining high security, usability, and compliance.

5.2 *MFA implementation approach effectiveness evaluation*

The suggested Multi-Factor Authentication (MFA) implementation technique improves network security. MFA successfully prevents illegal access by integrating passwords, fingerprints, and tokens. Data from the study process shows good results for security efficacy, compliance, and auditability. This shows that the MFA system can guard against cyber risks and meet regulatory requirements.MFA's versatility and scalability enable it to adapt to organizational demands and technology advances. The system's robustness and usability are improved by its dynamic authentication requirements depending on contextual elements and risk levels. MFA deployment approach maintenance and cost-effectiveness are good, with reasonable overheads and minimum operational interruptions.

Table 2

Summary of MFA implementation approach effectiveness evaluation

Parameter	Before IDPS	After IDPS	Resource Allocation
SQL Injection	80%	20%	70%
Cross-Site Scripting (XSS)	60%	30%	50%
Brute Force Attacks	80%	40%	60%
Denial of Service (DoS)	90%	30%	70%
Malware Infections	85%	15%	75%

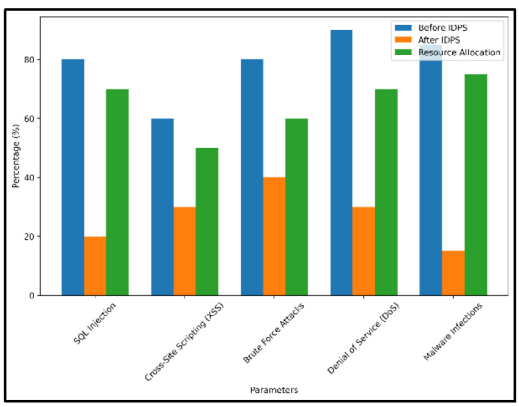

Figure 3

Impact of IDPS on Threats and Resource Allocation

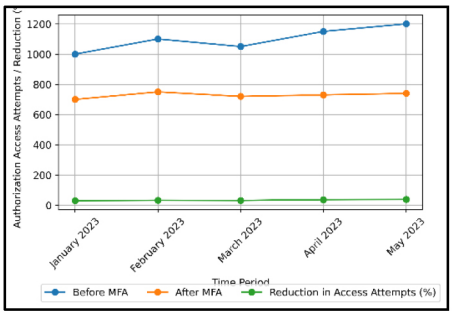

Figure 4

Impact of Multi-Factor Authentication (MFA) on Authorization Access Attempts

Table 2 summarizes the efficacy of Multi-Factor Authentication (MFA) in minimizing risks before and after IDPS deployment, along with resource allocation considerations. Post-IDPS deployment, threat intensity decreased across parameters. From 80% to 20%, SQL injection vulnerability drops, demonstrating considerable mitigation. XSS, Brute Force Attacks, DoS, and Malware Infections also decrease in severity following IDPS adoption. MFA and IDPS improve security against a variety of cyber attacks, as shown by this drop in Figure 3 and 4. Threat mitigation resources are allocated strategically, coinciding with threat intensity and possible effect on the organization's security posture

6. Conclusion

Using Multi-Factor Authentication (MFA) is a very important step for current businesses to take to make sure that only authorized people can access their networks. Multiple verification factors, like passwords, fingerprints, and keys, work together in multifactor authentication (MFA). This makes it very hard for people who aren't supposed to be there to get in. This study went into detail about how important MFA is and showed how well it works to stop possible risks and improve total security.The results showed how important it is to have a complete MFA plan that fits the needs of the company and takes into account things like usefulness, scale, and following all the rules set by regulators. The testing of MFA application showed that it worked the same way at different times, showing that it is resilient and can change to changing situations.The study also found important information about how well MFA works with

current security systems. This shows how important it is to keep an eye on things and evaluate them all the time to effectively deal with new threats. There were also suggestions made to make users more aware of MFA and speed up the process, which would improve security without affecting usefulness.

References

[1] F. Fan, S.-C. Chu, J.-S. Pan, C. Lin, and H. Zhao, "An optimized machine learning technology scheme and its application in fault detection in wireless sensor networks," *Journal of Applied Statistics,* pp. 1–18 (2021).

[2] X. Xue and C. Jiang, "Matching sensor ontologies with multi-context similarity measure and parallel compact differential evolution algorithm," *IEEE Sensors Journal,* vol. 21, no. 21, pp. 24570–24578 (2021).

[3] Limkar, Suresh, Ashok, Wankhede Vishal, Singh, Sanjeev, Singh, Amrik, Wagh, Sharmila K. & Ajani, Samir N. A mechanism to ensure identity-based anonymity and authentication for IoT infrastructure using cryptography, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1597–1611 (2023).

[4] T.-Y. Wu, L. Yang, Z. Lee, S.-C. Chu, S. Kumari, and S. Kumar, "A provably secure three-factor authentication protocol for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5537018, 15 pages (2021).

[5] M. J. Sadri and M. R. Asaar, "An anonymous two-factor authentication protocol for iot-based applications," *Computer Networks,* vol. 199, Article ID 108460 (2021).

[6] M.-S. Jian and J. M.-T. Wu, "Hybrid internet of things (iot) data transmission security corresponding to device verification," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–10 (2021).

[7] S. A. Chaudhry, A. Irshad, J. Nebhen et al., "An anonymous device to device access control based on secure certificate for internet of medical things systems," *Sustainable Cities and Society,* vol. 75, Article ID 103322 (2021).

[8] Ajani, S. N., Khobragade, P., Dhone, M., Ganguly, B., Shelke, N., &Parati, N. Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. *International Journal of*

Intelligent Systems and Applications in Engineering, 12(7s), 546–559 (2023).

[9] X. Xue and J. Chen, "Using compact evolutionary tabu search algorithm for matching sensor ontologies," *Swarm and Evolutionary Computation*, vol. 48, pp. 25–30 (2019).

[10] S.-C. Chu, T.-K. Dao, J.-S. Pan, and T. T. Nguyen, "Identifying correctness data scheme for aggregating data in cluster heads of wireless sensor network based on naive bayes classification," *EURASIP Journal on Wireless Communications and Networking,* vol. 2020, no. 1, pp. 52–15 (2020).

[11] G. T. Reddy, R. Kaluri, P. K. Reddy, K. Lakshmanna, S. Koppu, and D. S. Rajput, "A novel approach for home surveillance system using iot adaptive security," in Proceedings of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India (2019).