International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

A Survey and Critical Analysis of Multifactor Authentication Schemes in Modern ICT Environments

Ajit Singh, Bhumika

Assistant Professor, Department of Computer Engineering, The Technological Institute of Textile and Sciences, Bhiwani
Email: *ajitsingh[at]titsbhiwani.ac.in, Bhumika[at]ce.titsbhiwani.ac.in*

Abstract: ***With the rapid growth of distributed networks and ICT, online services have become widespread, raising critical concerns about authentication and data security. This paper surveys and analyzes multifactor authentication (MFA) schemes, highlighting the limitations of single-factor methods and the advantages of multifactor authentication schemes using passwords, smart cards, and biometrics. The current paper presents a systematic review of multifactor authentication schemes. Furthermore, the emphasis will also be laid on crucial findings that demand future addressal.***

Keywords: Single-factor authentication schemes, Multi-factor authentication schemes (MFA), Information and communication Technology

1. Introduction

With the rapid development in distributed networking and Information and communication Technology (ICT) has provided a scalable platform for various online services such as internet banking, electronic data interchange, secure e-commerce, online shopping, e-health etc., where users can interact with remote servers over an insecure public channel. The open transmission of data or services through insecure channel raises the imperative security challenges such as authentication, privacy and integrity. The recent advancement in network and processing power of digital machines escalates the possibility to a new kind of threat every day. To countermeasure all the associated challenges, network security has received a lot of attention these days [1-2]. According to Kalra & Sood [3], network security is a key domain where researchers have been rigorously working towards the goal of robust communication. There will always be a non ending race between the researchers and the attackers leading to a revolutionized invention and innovation in the field of network security.

In regard of the existing challenges of open networks and significant rise in online services, it become crucial to identify legitimate users and to stop intruders to access illegal web resources. Therefore, authentication mechanisms have become an essential aspect of network security. Authentication is a primary step before giving access to requested resources and to control most of the common attacks. Generally, there are two known authentication schemes: (1) Single factor-based authentication and (2) Multi-factor based authentication schemes. Single factor authentication schemes are mainly based on something that the user knows such as password. No doubt, it is simpler and cheaper method but password maintenance is a very big concern for system administrators. A study shows that system administrations spend about 40% of their time creating, resetting or changing user passwords. Apart from these issues, there are numerous attacks like stolen verifier attack, brute force attack, online and offline dictionary attacks, password inadequacy which make single factor-based authentication methods insecure and outdated where critical infrastructure and services demand adequate level of security [5-7].

In addition, multifactor authentication which gained a lot of momentum in authentication research field where at least two authenticating credentials are used out of three:

- What you know? e.g. password, pass phrases etc.
- What you possess? e.g. smart cards, certificates etc.
- What you are? e.g. biometric features such as iris, retina scan, fingerprint etc.

Numerous research has been carried out on smart card-based multifactor authentication schemes in which smart card is one of the essential authenticating credential factors. Smart cards are small plastic cards possessing small integrated chips having 4KB memory to store user parameters and process computational functions. They are secure, portable, and capable of mutual authentication between users and remote servers. The primary objective of these schemes is to verify the legitimacy of the communicating parties and withstand adversarial attacks. Therefore, smart card-based multifactor authentication schemes are robust and efficient enough to meet the requirements of a modern computing environment and ever-increasing security threats [8–10].

2. Literature Review

This section summarizes related works and evaluates existing authentication schemes in the context of current research challenges.

Mishra et al. (2015) designed a password-based authentication scheme to establish a secure and authorized communication between the remote entities over the insecure public network. They addressed that existing scheme does not satisfy the desirable attributes such as resistance against various known attacks and the user anonymity. Performance analysis shows that it is efficient in terms of computational and communication overheads. Also,

Paper ID: SR25608215420 DOI: https://dx.doi.org/10.21275/SR25608215420

simulation using AVISPA tool ensures completeness and resistance against active and passive attacks [7].

Mishr and Barnwal (2015) designed a privacy preserving authentication scheme for Telecare Medicine Information System to achieve eminent security in the consent of patient privacy. The authors highlight and erase security related pitfalls by adding a new concept of pre-smart card authentication, which results user login and change their password without server assistance [8].

Reddy et al. (2016) presented a secure anonymous authentication protocol due to the greater deployment of handled devices and advanced e-technologies. The proposed protocol used lightweight operations such as Elliptic Curve Cryptography, Elliptic Curve Diffie Hellman, and Elliptic Curve Digital Signature Algorithm etc. During authentication which ensures it is significant towards resource constrained environment. The informal and formal security analysis demonstrates the resistance against all sorts of security attacks [9].

Kumar et al. (2016) presented a password based authenticated scheme to remove the weakness of multi-server authenticated scheme, which usually adopts the architecture of two-level servers. The major advantage of this proposed scheme is provably secure under the Chebyshev Diffie Hellman assumption of Chebyshev polynomial in the random oracle method. Furthermore, it improves the performance of the registration authentication phase and preserves user privacy [10].

Ometov et al. (2018) designed a user anonymous authentication scheme for Telecare Medicine Information. The author addressed user anonymity, stolen card attack, offline & online password guessing attack etc. in the existing related scheme. BAN [40] analysis of this scheme ensures the completeness and correctness of the designed scheme. Finally, formal security analyses verify that it is safe against active and passive attacks [11].

Singh et al. (2019) designed a lightweight and energy efficient authentication scheme for resource constrained environment. The authors used the concept of low-cost cryptographic primitives such as one way hash function and Exclusive-OR operation to accomplish goals. The formal and informal analysis depicts that scheme is suitable for low power mobile device in a hostile environment [13].

Wang et al. (2020) designed a secure lightweight scheme for user authenticated in battery constrained environments. Performance analysis ensures that the energy consumption of the sensor node should be minimum to increase the lifetime of network. Additionally, the scheme also achieves an efficient login phase, user friendly, password update phase, proper mutual authentication, strong security protection on the session key and dynamic node addition which make it more efficient for battery constraint devices [14].

Fakroon et al. (2021) designed a secure and robust user authenticated key agreement scheme in order to erase several security drawbacks and design flaws found in Amin-Biswas's scheme. Performance and functional analysis indicate that this scheme provides more features and is efficient in terms of communication and computation cost. The author has also showed rigorous formal security analysis using BAN logic and random oracle method to ensure robustness against various known attacks [15].

Tahir et al. (2023) proposed a robust biometric based authentication scheme to ensure seamless and secure services to the remote user; such services espouse authentication protocols. The analysis confirmed that the proposed scheme achieves mutual authentication and is robust against known attack without incurring any extra computation cost [17].

Syahreen et al. (2024) gives comment on efficient and secure dynamic Id based authentication and puts forth some of the design flaw in user registration and password change phase, which leads to failure in mutual authentication process. The author also observed flaws in the pre-image resistance property of one-way hash function [19].

Ang et al. (2025) designed a secure smartcard based multi-server authentication to provide a scalable solution in personal and ubiquitous computing technologies. The scheme worked on previously related problems which involve control servers in mutual authentication and their related security pitfalls. The authors also countermeasure all these issues using the concept of biometric credentials during authentication. Performance analysis depicts that the scheme is efficient in terms of computational and communicational overheads [20].

3. Crucial Findings

Having a critical examination at the available literature review, it can be concluded that due to recent advancements in Information and communication Technology (ICT), have revolutionized the quality of online services in distributed environment such as online banking, e-commerce, e-medicine, e-health, online shopping etc. This provides a unique opportunity for a user to interact with servers over insecure channels. Therefore, the design and analysis of multifactor authentication scheme have received considerable attention for research nowadays.

Conventional single factor-based authentication techniques such as password authentication schemes are not suitable for today's environment due to increase in the availability of processing power machines and numerous attacks like stolen verifier attack, brute force attack, online and offline dictionary attacks, password inadequacy. While multifactor authentication schemes provide robust security as compared to single factor due to subsequent addition of credentials authentication factors. Even with significant advancements, there are still several important issues that need to be addressed, providing plenty of opportunity for further study. Important concerns include:

1) More emphasis on eminent security and efficiency of authentication schemes need to be provided.
2) Computational and communication overheads need to be decreased.

3) Strong replay attack, stolen smart attack, user verification table attack, user and server anonymity, man in middle attack, scalability of login, proper authentication phase, denial of service attack, user impersonation attack, server impersonation attack, privileged insider attack, freedom of password and biometric update, password guessing attacks, no user revocation phase etc. are still critical attacks in existing schemes. Although some schemes claim resistance to these threats, many are still vulnerable under alternative threat models.
4) Scalability of login in multi-server environment need to be explored.
5) Flaws in the design of login, authentication and password update phases need to be addressed.
6) Rigorous formal and informal security analysis using different threat models and validation tools need to be carried out.

4. Conclusion

This paper presents a comprehensive survey and critical analysis of multifactor authentication (MFA) schemes within modern ICT environments. With the increasing reliance on distributed networks for online services, the inadequacy of single-factor authentication methods has become apparent. MFA schemes, integrating credentials like passwords, biometrics, and smart cards, offer enhanced security. However, despite notable advancements, existing schemes still face challenges including high computational overhead, vulnerability to sophisticated attacks, and poor scalability in multi-server environments.

The study underscores the necessity for future research to focus on lightweight, scalable, and resilient authentication frameworks. Emphasis should also be placed on formal and informal security validation and practical deployment strategies. Ultimately, the secure implementation of multifactor authentication schemes remains a critical area for ongoing exploration in ensuring robust user authentication across evolving ICT infrastructures.

References

[1] Gope P., “Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks”, IEEE Systems Journal, 2015.
[2] Das A. K., Odelu V. and Goswami A., “A Secure and Robust User Authenticated Key Agreement Scheme for Hierarchical Multi-medical Server Environment in TMIS”, Journal of Medical Systems, 2015.
[3] Kalra S., and Sood S. K., “Elliptic Curve Cryptography Based Password Authentication Protocols”, 2014, http://shodhganga.inflibnet.ac.in/handle/10603/97374.
[4] Biswa G. P. and Amin R., “A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks”, Journal of Adhoc networks, 2015.
[5] Kumari S., Khan M. K. and Atiquzzaman M., “User authentication schemes for wireless sensor networks: A review”, Ad Hoc Networks, 2015.
[6] Nash, Andrew et al., PKI- Implementing and Managing E-security, Tata McGraw-Hill, 2000.
[7] Mishra D., Das A.K., Mukhopadhay S. and Wazid M., “A Secure and Robust Smartcard-Based Authentication Scheme for Session Initiation Protocol Using Elliptic Curve Cryptography”, Journal of Wireless Pers Communication, 2015.
[8] Mishra R. and Barnwal A. K., “A Privacy Preserving Secure and Efficient Authentication Scheme for Telecare Medical Information Systems”, Journal of Medical Systems, 2015.
[9] Reddy A. G., Das A. K., Yoon E. J. and Yoo K. Y., “A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography, IEEE Transactions, 2016.
[10] Kumar R., “A privacy preserving multi-server authenticated key agreement scheme based on chebyshev chaotic map” Security and communications networks, 2016.
[11] Ometov, A., “Multi-factor authentication: A survey”, Cryptography, 2018.
[12] Dhillon, P. K., and Kalra S., “Multi-factor user authentication scheme for IoT-based healthcare services”, Journal of Reliable Intelligent Environments, 2018.
[13] Singh C. and Singh D, “A 3-level multifactor authentication scheme for cloud computing”, International Journal of Computer Engineering and Technology, 2019.
[14] Wang D., “Understanding security failures of multi-factor authentication schemes for multi-server environments”, Computers & Security, 2020.
[15] Moneer F., Gebali F. and Mamun M, “Multifactor authentication scheme using physically unclonable functions”, Internet of Things, 2021.
[16] Khan, A. S., “Lightweight multifactor authentication scheme for next generation cellular networks”, IEEE access, 2022.
[17] Tahir, H., “Lightweight and secure multi-factor authentication scheme in VANETs”, IEEE Transactions on Vehicular Technology, 2023.
[18] Kumar, R., Singh S. and Singh P. K., “A secure and efficient computation based multifactor authentication scheme for Intelligent IoT-enabled WSNs”, Computers and Electrical Engineering, 2023.
[19] Syahreen M., “A Systematic Review on Multi-Factor Authentication Framework”, International Journal of Advanced Computer Science & Applications, 2024.
[20] Ang K. W., “Unveiling the Covert Vulnerabilities in Multi-Factor Authentication Protocols: A Systematic Review and Security Analysis”, ACM Computing Surveys, 2025.