Abstract

With the rise of escalating cyber threats to the present-day networking environment, the traditional two-factor authentication (2FA) mechanisms remain ineffective in mitigating the sophisticated attack vectors like phishing, SIM-swapping and social engineering. These loops holes, specifically in SMS- and email-based 2FA, are opening users and network infrastructure up to substantial danger. This paper presents optimized and robust enhancements to 2FA technology, and points out cryptographic technologies like ECC, the addition of X.509 digital certificates, and biometric and behavioral authentication solutions. Then, the performance of these distributed trust models is compared, in terms of security efficiency, usability, and deploy ability, with a complete comparative study of these models in dynamic networking. The paper also includes real-world examples of implementing such multi-layered 2FA schemes being tensioned between a strong security protection and what is deemed to be user acceptable. The results showcase best practices and challenges in building secure and efficient as well as future-proof authentication systems that match the requirements of complex network environments.