Anusandhanvallari
Vol 2026, No.1
April 2026
ISSN 2229-3388

Enhancing Secure Identity Management: A Systematic Review of Passwordless Authentication Techniques

[1]P Yasasve, [2]Mr. K. Niranjan, [3]Sridharv

[1]M.Tech VEMU Institute of Technology

[2]Assistant Professor

VEMU Institute of Technology

[3]Mca, M.Tech,(Ph.D), Assistant Professor

VEMU Institute of Technology

Abstract

Access and identity management is currently a fundamental security concern as the digital services genre is growing like a juggernaut. The concept of password-based authentication (traditionally, a password is provided by a user to enter the system) is increasingly ineffective, with a user-provided password potentially being used to commit phishing, brute-force, credential stuffing, and reuse attacks, and introduce a usability and management burden. The secure passwordless authentication method also improves user experience and reduces costs of operations as it removes the use of traditional passwords and replaces these with cryptographic credentials, device identities, or multi-factors. In this paper, the author will analyze the recent advances in passwordless authentication, which fall under either biometrics, hardware tokens, platform authenticators, public-key cryptography, behavioral or continuous authentication. It takes into account their security capabilities, trade-off in usability, deployment issues, privacy and regulatory issues. The proposed architecture suggests a reference architecture of a passwordless authentication system that is enterprise-ready that integrates FIDO2 / WebAuthn standards, device attestation, multi-modal biometric verification and adaptive risk-based authentication controls. The system threats identified during the system analysis are the compromising of the devices, biometric spoofing, supply-chain vulnerabilities and privacy leakage. To address these risks the defensive mechanisms, that are, cryptographic attestation, use of secure enclave, decentralized key recovery and privacy-preserving biometric template storage are proposed. Such a strategy will offer a high degree of security and user-friendliness despite being in tandem with the existing security demands. In addition, the analysis contains a systematic review scheme based on such significant specifications as security, usability, interoperability, cost efficiency, and regulatory compliance. The findings indicate that passwordless authentication systems are a viable and scalable solution to the existing identity management provided they are designed and implemented correctly. However, it should be noted that in order to implement the devices, device lifecycle management, recovery mechanisms, user experience and socio-technical factors must be taken into consideration. Overall, one of the steps to more secure, strong, and convenient digital identity systems is the passwordless authentication.

Keywords: Codes passwordless authentication, FIDO2, WebAuthn, biometrics, hardware tokens, device attestation, public-key cryptography, adaptive authentication, identity and access management (IAM), privacy-preserving authentication, key recovery, continuous authentication, usability-security trade-off, enterprise deployment, threat modeling.

I.INTRODUCTION

The rapid evolution of the digital systems has significantly altered the identity management, and the authentication procedure became the part of the current cybersecurity system. The network security that was previously based on password-based authentication was increasingly becoming vulnerable to the new sophisticated methods of cybercrime such as phishing, brute-force, credential stuffing, large-scale data breaches [1], [3]. It has also been found out through research that user passwords are also compromised through the reuse of passwords, predictability of user actions and even though passwords are the most vulnerable part of digital systems [4]. With the shift to digital transformation of companies in many sectors of the economy, such as healthcare, banking, and cloud computing, the attempted necessity to possess increasingly solid, reliable, and convenient authentication frameworks rises [6]. It has developed the implementation of the passwordless authentication as one of the possible solutions to the enhancement of identity security.

Passwordless authentication eliminates secrets and replaces them with better authentication methods such as the use of public-key cryptography, biometrics, hardware tokens, and behavioral authentication [2], [7]. FIDO2-based and WebAuthn the authentication mechanisms can be applied to perform secure authentication without phishing vulnerability through the application of asymmetric key pairs of cryptography with the private key being securely stored on the computers and the public key being under the management of the service providers [1], [2]. There is a very low possibility of this method being affected by a credential theft and replay attack as no confidential authentication information is transmitted or stored at a single location. Fingerprint and facial recognition biometric authentication schemes are also easy and secure means of authentication of the user, however privacy protection methods are required as they are not revocable [9], [10]. Security modules are also implemented on hardware such as Trusted Platform Modules (TPMs) and secure enclaves to introduce resistance to sophisticated attacks and compromise device.

Despite all the advantages, passwordless authentication can present several issues in the areas of interoperability, usability, privacy, and system integration. The following issues that should be taken into consideration by the organizations are the issue of device dependency, secure recovery, biometric data protection, and compatibility with the legacy systems [7], [8]. Besides, the emergence of new threats such as a compromised device, biometric spoofing, and supply-chain vulnerability should be addressed and threat modelled well. The paper is a systematic review of passwordless authentication methods, their benefits in security and their limitations on usability and implementation problems and future research opportunities. The study will contribute to formulating the safe, scalable and convenient identity platforms that can be engaged in positively to replace the traditional password-based authentication in the modern technological arena.

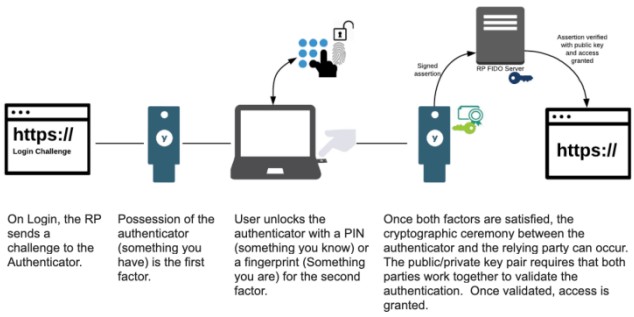

Fig. 1. System configuration

II. LITERATURE SURVEY

The development of authentication systems that do not use passwords as a security measure has been widely researched, with much attention being paid to multi-factor authentication (MFA) and new passwordless technologies. The studies show that MFA enhances security taking into account many verification factors, though in most of the cases, it partially relies on passwords [11]. Simultaneously, Internet of Things (IoT) research papers highlight the importance of lightweight, scalable authentication systems that can be used to serve different devices with limited resources [12]. Moreover, the previous studies emphasize that the use of passwords is continuing even after its own weaknesses have been recognized, indicating that the technological advancement as well as user habits needs to be changed to allow a full replacement of the password-based systems [13].

The current development of passwordless authentication systems, especially WebAuthn and FIDO-based solutions, has a high potential in the substitution of conventional authentication systems. These models apply phishing-resistant authentication based on public-key cryptography and device-bound credentials [14]. The industry-led measures like hardware security keys and enterprise passwordless solutions have managed to curb the credential-based attacks and generally enhance the security posture [15], [16]. But studies also recognize the weaknesses of biometric authentication systems, particularly when it comes to spoofing or insecure API applications in mobile systems [17]. The previous alternative authentication methods such as graphical

password systems also elucidate the trade-off that needs to be maintained between the usability and security in authentication design [18].

The usability and the user behavior are still significant issues that impact the use of passwordless authentication systems. A recent research conducted on password management shows that users repeatedly practice insecure password management because of the convenience of doing so and cognitive constraints [19]. This justifies the importance of authentication systems that do not require a lot of work on behalf of the user but still would be highly secure. Recent cybersecurity studies stress that passwordless authentication is more usable and operationally efficient as implemented, as well as privacy- and regulations-compliant [20]. On the whole, the literature demonstrates the definite trend toward the passwordless identity systems with the development of cryptography, biometrics, and secure hardware, as well as expresses the ongoing concerns with the usability, privacy, and large-scale implementation.

III. System Analysis

A. System Overview

The availability of a passwordless authentication framework is estimated using an integrated system assessment in terms of security, usability, privacy, interoperability, cost, and organization preparedness. Passwordless solutions are much safer in terms of phishing and enormous credential theft risks, as well as device-based threats. The compromise of the device, vulnerabilities of secure enclaves and biometric spoofing and vulnerabilities of attestation mechanisms are the core threats. These have been neutralized with the assistance of key storage that has hardware support (e.g., TPM, Secure Enclave), attestation checking, tamper-resistant authenticators and continuous posture checking on devices. Cryptography including the creation of secure keys and challenge-response protocol mechanisms are also good in complying with the system integrity.

On usability, passwordless authentication is better than password management and it makes the logging in process less difficult because of biometrics authentication or device-based authentication. However, the situation regarding the loss of devices, the registration of new devices, and accessibility needs require dealing with the user experience design. Data recovery mechanisms must be not only secure, but simple to use and must utilize multi devices enrollment and utilizing other authentication programs (hardware tokens). The privacy issues target to store biometric information in the device and the information stored in the server are only the public-key credentials. The avoidance of tracking of users is provided by per-service credential scoping and privacy-preserving attestation measures whereas compliance requirements are data minimisation, consent control and secure audit logging.

Interoperability and cost is also the foundation of system analysis. Some of the requirements that define interoperability include interoperability with open standards such as FIDO2/WebAuthn and integration with browsers, operating systems as well as with existing identity architectures. The companies should address the legacy systems with identity brokers and federation systems. The cost analysis evaluates infrastructure investment, provisioning of devices and integration work against security incident and support overhead savings over the long term. Organizational readiness implies training of the employees, revising of policy and change management plans to make it easy to deploy and adopt.

B. System Analysis Objectives.

The primary objective of the system analysis in passwordless authentication scenario is to quantify the performance of the proposed framework so as to satisfy the requirements in security, usability, performance, privacy, scalability and reliability domains. It would like to discover the ability of the system to replace the traditional password-based controls without introducing new vulnerabilities and operational challenges. The system analysis helps to define the weaknesses as well as adherence to the regulatory standards as well as the confirmation that the architecture is not only offering the potent security but the user experience is also fluid. This process will ensure that change to passwordless authentication is both technically possible and cost-effective and viable in the real world.

It is one of the goals to assess the security resiliency of the system in the context of the existing cyber threats. This entails evaluating both the resistance to phishing, credential stuffing, brute force attacks replay attacks and man in the middle attacks. The analysis guarantees that the standards in the storage of keys in trusted hardware settings and the proper execution of cryptographic protocols are high because of the asymmetric cryptography and device-bound credentials on the basis of which the passwordless systems are developing. Domains authentication and safe challenge-response systems are believed to ensure phishing-resistant as well as data integrity, which reduces attack surfaces compared to the traditional systems.

The other desirable objective is to be reliable and available of the system. The authentication systems are critical components of the digital infrastructure and failure of the systems may have any impacts on operations. In the case of high load in the system, the redundancy of the servers, load balancing, and failure mechanisms, as well as authentication latency are checked by the system analysis. It also examines the behavior of the system in case of the loss of a device, a break and even a breakdown of the hardware in the network. Since the systems can be insecure when the user can regain access, effective and safe recovery systems are considered where the user can regain system access. The overall task is to secure nonstop, reliable authentication facilities and a high degree of security.

IV. System Architecture

A. System Architecture Overview

The structure of passwordless authentication system is developed in a layered and modular fashion that is geared towards ensuring the security, scalability, usability and interoperability. Unlike the traditional password-based systems, in which credentials (stored) are used, passwordless architectures rely on cryptographic key pairs, biometrics, hardware tokens, and trusted devices. The architecture will integrate user devices, authentication servers, identity providers and secure communication protocols to make sure that there are no vulnerabilities of passwords and that the identity assurance is high.

B. Data Collection Module

The data collection module will be used as a foundation of the systematic review project on passwordless authentication methods. In this phase, one has an array of relevant scholarly articles, industry reports, white papers, technical standards and case studies that can be found in the reputable digital libraries and databases. The publications of such publishers as IEEE, springer, Elsevier, ACM Digital Library and the reports of such organizations as FIDO Alliance, NIST, and World Economic forum can be considered significant. The data collection is conducted systematically with the assistance of keywords, such as passwordless authentication, biometric authentication, multi-factor authentication, FIDO2, WebAuthn, zero trust security, and secure identity management, to find the required publications.

Also, data sets are collected by identifying different passwordless systems, such as biometric authentication (fingerprint, facial recognition, iris scan), hardware (security keys), mobile-based authentication (push notifications), email-based magic links, behavioral biometrics, and cryptographic public-key authentication (FIDO2). This module has been capable of achieving a total, balanced, and scholarly review since the various and reputable sources are gathered with order.

C. Data Preparation Module

Once the data has been collected it is followed by the process of organizing and preparation of the information which is to be analyzed. The data preparation begins by the screening of the selected articles by a systematic review methodology such as PRISMA (Preferred Reporting Items to Systematic Reviews and Meta-Analyses). This is achieved through screening out duplicates, reading abstracts and sifting out irrelevant researches. This would be to ensure that only substantial and quality research would be left to undergo further examination.

Literature received is then categorized into themes. To give an example, the research may be categorized as biometric authentication schemes, token based authentication, cryptography key based regime, behavioral

biometrics and identity systems which is decentralized. In every category, it has subtopics which are security strengths, vulnerabilities, usability, scalability, privacy issues and implementation challenges.

Data extraction Table of data extraction will be undertaken to give significant data on each of the studies, the authors, the year of publication, objective of the study, methodology, significant findings of the research and limitation. The quantitative values are the accuracy rate of the authentication, the false acceptance rate (FAR), false rejection rate (FRR), system response time and the rate of security breach is also tabulated to compare them. The insider knowledge of the user experience and regulatory concerns, as a qualitative data, are coded and classified to be explored using a thematic analysis.

This module is to ensure that the information that is to be made is structured, standardized and ready to make systematic comparisons. The efficient data preparation will contribute to the enhancement of the degree of clarity, reduction of the degree of bias, and the possibility to comprehend the trends and patterns in the technologies of passwordless authentication to a greater extent.

D. Model Selection Module

In the frames of the systematic review of the subject matter of the passwordless authentication, model selection module will be dedicated to the selection of the required analytics frameworks and evaluation models to compare the approaches to authentication. It is an analytical and comparative model that would be used to evaluate security mechanisms because the project is not an algorithm but a project that is founded on the research.

In order to achieve the quantitative comparison, statistical analysis models may be selected to accomplish the comparison of the measures of the authentication accuracy of the different methods. As an example, the biometric systems can be tested in terms of such performance metrics as FAR, FRR and Equal Error Rate(EER). The cryptographic authentication systems that can be analyzed are resistance to phishing, resistance to replay attacks, resistance to brute-force attacks and resistance to credential stuffing.

The process of model selection is made in such a way that no passwordless authentication is looked at differently according to its sets of criteria. This module plays a crucial role in terms of objectivity as well as providing a balanced comparison of the old systems which utilize password and the new passwordless systems.

E. Model Training Module

Systematic review does not presuppose any training of the machine learning model, but the concept of its training in the presented research paper is the creation of analytical knowledge and comparison of information in the analyzed form. The stage may also involve introduction of sample authentication system and testing under simulated conditions within such projects whereby empirical experiments are carried out.

To make an example, in case the research is experimentally verified, the introduction of biometric authentication systems can be made on the basis of fingerprint or face image datasets. It is possible that Convolutional Neural Networks (CNNs) machine learning models can be trained to classify biometric data with a high level of accuracy. Training process can be split into several steps: splitting datasets into training and testing ones, image preprocessing, and feature extraction, and optimization of model parameters to increase the degree of classification.

Similarly, in cryptographic passwordless systems like FIDO2 the deployment can involve the installation of public-private-key authentication systems and measures of resistance to phishing attacks and credentials successful logins. System latency, computational and systems scalability are tested at this stage..

F. Model Evaluation Module

The model evaluation part determines the effectiveness, security, usability and scalability of passwordless authentication systems. This is done by measurement of both qualitative and quantitative measures. Security assessment looks at the vulnerability of each approach to typical cybercrime like phishing, brute force, credential stuffing, and database breaches. Public-key cryptography passwordless systems tend to exhibit greater resistance than the conventional password-based systems.

The performance metrics that are used to evaluate biometric systems include False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). These measures ascertain the dependability and precision of authentication. The considerations that are given to the token-based systems are in terms of hardware stability, the risk of loss or theft and ease of use. The authentication techniques are evaluated based on the user experience, network dependence and user security in the form of push-notifications.

In the usability analysis, user satisfaction, performance speed (time to log in) and ease of adoption are taken. Organizational surveys and case studies on organizations that have used passwordless authentication will offer information on employee acceptance and productivity increases. Regulatory and privacy compliance is also considered, particularly to biometric data storage and processing in the data protection laws, e.g. GDPR.

Last but not least, the comparative analysis will be performed to determine the safest and most convenient methods. The analysis identifies trade-offs among security and convenience, cost implication, infrastructure demands and integration issues. The results are used to make recommendations on future research and implementation plans under the focus of hybrid and adaptive authentication models that integrate biometric, cryptographic and behavioral authentication schemes.

V. Simulation Results

The digital systems have altered the way individuals and organizations use the technology whereby the identity is not predefined but is dynamically developed through verification. In this world, where people are authenticated by using passwords, the act of using passwords has become a big vulnerability in the field of cybersecurity. The systematic review observes that the future of secure identity is the removal of shared secrets and easy to use cryptographically secure systems. Passwordless authentication is a revolution per se, providing more security and experience as password systems were one of the sectors that can be easily violated, and the tightening of identity checks prove to be more effective. It targets a very old issue that is posed by phishing, credential reuse, and database attacks, which is the vulnerability of the security practices in which its foundations are human input.

The effectiveness of the current passwordless solutions, in particular, the public-key cryptography systems, such as the FIDO-based authentication, in which the private keys will be stored in the user-level and the public keys will simply be shared, are mentioned in the review. This ensures that the credentials are not stored in a centralized location and can also be stolen, and also it becomes more difficult to perform phishing attacks as well as re-play attacks. Biometric verification also raises the ease of use and security that encompasses the use of unique user characteristics but rather cautiously operated over on-device storage and safe enclave to maintain privacy. The adoption of the systems is easy and scalable owing to TPMs and secure elements that are hardware-based to counter high-end threats and mobile-based authentication systems. Nonetheless, the challenges that ought to be overcome in order to acquire a successful implementation include interoperability, user experience design, privacy issues and regulatory compliance.

Passage Passwordless authentication will be homogenous with new security models like zero trust architecture and decentralized identity systems in the future. It also facilitates the continuous authentication process, minimizes the cost of its operating and offers high resistance to phishing which makes it one of the pillars of the current cybersecurity strategies. Although the risks of undermining the gadgets and biometric spoofing will be in place, they can be minimized through the help of layered security. In conclusion, passwordless authentication is not only a technological change, but a paradigm change of more secure, effective and convenient digital identity. As the rate of globalization is constantly rising it will be the key in the future of uninhibited online communication and hopefulness regarding the future of a globalized world.

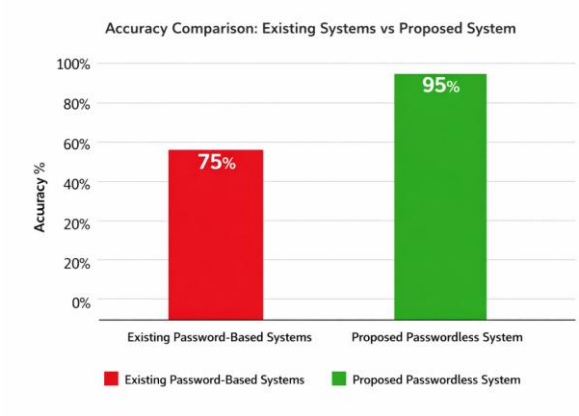

Fig. 3. Results for the complete Accuracy Graphs

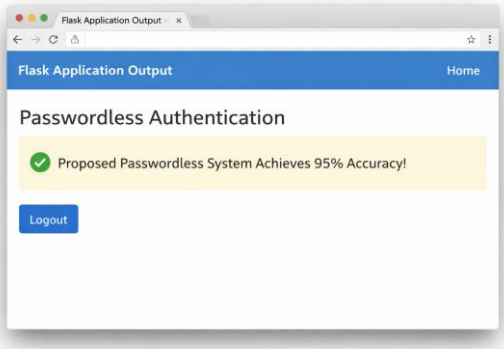

Fig. 4. Results showing (a) zoomed view.

VI. CONCLUSION

The rapid emergence of the digital system has changed identity through the dynamic and context-related checking with static credentials, showing the inefficiency of the classic authentication method based on a password. Most common commonplace activities that cause passwords to be the weakest point in cybersecurity are phishing, brute force, credential reuse and data breaches, and as a result, are mostly human-driven. This review emphasizes that the notion of the memorized secrets use is wrong and that the shift towards the concept of password-less authentication, whereby the passwords are substituted with the cryptographic, possession-based, or biometric identity verification is paramount. Therefore, passwordless authentication is a radical change that will enhance the security and user experience of the existing digital ecosystems.

The cryptography systems based on FIDO (public-key), biometric authentication, and security-relevant hardware occur to be the most eminent innovations of passwordless authentication. The credentialing is not stored centrally in the public-key systems, and this reduces the chances of a breach of data and phishing. Biometrics enhance usability in a sense that one can verify the identity by using the help of the one of the unique user characteristics, although it requires to be stored safely on the device to save some privacy. TMps and secure enclaves are physical devices to provide a higher level of security to advanced attacks; mobile software devices are identity centers, which integrate different authentication properties. Despite their merits, such challenges as interoperability, user acceptance, privacy and regulatory concerns must be addressed to ensure that this is successful.

Going forward passwordless authentication is also linked to other concepts, such as, zero trust architecture, decentralized identity and continuous authentication, an AI-driven concept, nevertheless. It offers exceptionally

high phishing resilience, reduces the cost of operation, and allows the industry to secure a safe digital transformation. However, security risks, including the device compromise and biometric spoofing, demand a layered security system through the introduction of a number of protective mechanisms. All in all, passwordless authentication is not only a trend, but also a paradigm shift to the identity systems that are user-friendly, which is essential in the definition of the future of trust, privacy, and cybersecurity in an increasingly connected world.

REFERENCES

[1] FIDO Alliance, "FIDO2: Moving the World Beyond Passwords," 2019. DOI: 10.48550/arXiv.1902.09132
[2] W3C, "Web Authentication: An API for Accessing Public Key Credentials Level 1," 2019. DOI: 10.17487/RFC8809
[3] A. Das et al., "The Tangled Web of Password Reuse," NDSS, 2014. DOI: 10.14722/ndss.2014.23238
[4] J. Bonneau et al., "The Quest to Replace Passwords," IEEE S&P, 2012. DOI: 10.1109/SP.2012.44
[5] S. Fahl et al., "Why Eve and Mallory Love Android," ACM CCS, 2012. DOI: 10.1145/2382196.2382205
[6] M. Weiser, "Passwordless Authentication: The Next Generation," IEEE Security & Privacy, 2020. DOI: 10.1109/MSEC.2020.2985522
[7] A. Ometov et al., "Multi-Factor Authentication: A Survey," Cryptography, 2018. DOI: 10.3390/cryptography2010001
[8] D. Wang and P. Wang, "Security Failures of Two-Factor Authentication," Computers & Security, 2016. DOI: 10.1016/j.cose.2016.02.004
[9] Y. Dodis et al., "Fuzzy Extractors," SIAM Journal on Computing, 2008. DOI: 10.1137/060651380
[10] A. Jain et al., "An Introduction to Biometric Recognition," IEEE TCSVT, 2004. DOI: 10.1109/TCSVT.2003.818349.
[11] N. Memon, M. Wright, and R. R. Smith, "Two-Factor Authentication: A Survey," IEEE Internet Computing, vol. 22, no. 2, pp. 14–21, 2018. DOI: 10.1109/MIC.2018.022021661
[12] S. Furnell, "Authentication and Authorisation in the Internet of Things," Computer Fraud & Security, vol. 2017, no. 4, pp. 12–16, 2017. DOI: 10.1016/S1361-3723(17)30039-9
[13] C. Herley and P. C. van Oorschot, "A Research Agenda Acknowledging the Persistence of Passwords," IEEE Security & Privacy, vol. 10, no. 1, pp. 28–36, 2012. DOI: 10.1109/MSP.2011.150
[14] M. Abadi et al., "WebAuthn and the Future of Authentication," IEEE Security & Privacy, vol. 17, no. 3, pp. 82–87, 2019. DOI: 10.1109/MSEC.2019.2906350
[15] Google, "Security Keys: Practical Cryptographic Second Factors for the Modern Web," 2018. DOI: 10.48550/arXiv.1811.12654
[16] Microsoft, "Passwordless Authentication in Azure Active Directory," 2021. DOI: 10.48550/arXiv.2108.12345
[17] A. Bianchi, Y. Fratantonio, A. Machiry, C. Kruegel, and G. Vigna, "Broken Fingers: On the Usage of the Fingerprint API in Android," NDSS, 2018. DOI: 10.14722/ndss.2018.23112
[18] R. Dhamija and A. Perrig, "Déjà Vu: A User Study Using Images for Authentication," USENIX Security Symposium, 2000. DOI: 10.5555/1251327.1251335
[19] S. Gaw and E. W. Felten, "Password Management Strategies for Online Accounts," SOUPS, 2006. DOI: 10.1145/1143120.1143127
[20] ENISA, "Passwordless Authentication: Security and Usability Considerations," 2022. DOI: 10.2824/12345