Volume: 16 Issue: 02 Pages: 6349– 6355 (2024) ISSN: 0975-0290

Security Reinforcement: An Overview of Multilevel Authentication Techniques

Ts.Dr. Thamilvaani Arvaree @ Alvar
Faculty of Science and Engineering, University of Nottingham Malaysia, Jalan Broga, 43500 Semenyih, Selangor Darul Ehsan, Malaysia
Email: Thamil.Vaani@nottingham.edu.my
ORCID iD: https://orcid.org/0000-0002-7292-5075

ABSTRACT

Authentication mechanisms play a critical role in safeguarding against unauthorized access in today's mobile operating systems. This paper presents a comprehensive review of existing authentication methods tailored for mobile devices, aiming to elucidate their functionalities and security considerations. The study meticulously examines a spectrum of authentication techniques available for smart devices, shedding light on their respective features and implementation within mobile operating systems. Additionally, it scrutinizes the associated security risks specific to these methods. By providing an in-depth analysis of prevalent authentication approaches, this research aims to offer valuable insights into the landscape of available techniques for securing mobile devices, aiding both users and practitioners in making informed decisions regarding their adoption.

Keywords- **Authentication, multi-level authentications, mobile devices**.

Date of Submission: June 24, 2024 Date of Acceptance: Aug 02, 2024

I. INTRODUCTION

The advent of mobile phones primarily aimed to revolutionize communication, but the evolution into smartphones has transformed them into multifaceted devices facilitating a wide array of activities, from communication to complex online transactions. With this evolution, concerns surrounding data security have intensified, prompting the development and implementation of diverse authentication methods to fortify protection against unauthorized access.

Conventional email/password-based authentication remains ubiquitous, yet a spectrum of authentication modalities has emerged, encompassing knowledge-based (e.g., passwords), biometric (e.g., fingerprints), and ownership-based (e.g., USB tokens) methods. However, widespread adoption of biometric authentication in mobile applications remains limited due to hardware constraints across devices, and ownership-based authentication faces challenges due to specific hardware requirements. Each authentication type presents unique advantages and limitations, encompassing factors like cost, ease of use, and varying levels of security. Surveys have highlighted that a substantial majority of users recognize the sensitive nature of data stored on their mobile devices, fostering a growing emphasis on fortifying security measures. Notably, the prevalence of password sharing has exposed vulnerabilities associated with single-factor authentication, prompting a pivot toward more robust methods like Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) as viable solutions.

Despite heightened awareness of security issues, there exists a gap between understanding and implementation among users. While acknowledging the importance of security measures like 2FA, some users remain hesitant to activate these features due to perceived complexities or inconveniences, underscoring the ongoing challenge of balancing security and usability. In this paper, a comprehensive comparison and analysis of diverse authentication types and techniques applicable to a wide range of mobile devices are conducted. The examination aims to elucidate the efficacy, usability, and feasibility of these methods in securing mobile devices, thereby offering valuable insights for both users and developers navigating the evolving landscape of mobile security.

II. LITERATURE REVIEW

Authenticating users and verifying their identities holds paramount importance in numerous mobile applications, particularly those involving online transactions and sensitive data access. Various methodologies exist to establish user identity and access. For instance, the classic username and password combination represents a knowledge-based authentication method, requiring users to input familiar information for verification. Additionally, ownership authentication utilizes tangible objects like a smart card or User ID Card, granting access to physical spaces or systems, categorizing this method as ownership-based authentication. Furthermore, biometric authentication offers a third avenue, relying on unique biological characteristics, such as fingerprints, to authenticate users based on who they are.

Volume: 16 Issue: 02 Pages: 6349– 6355 (2024) ISSN: 0975-0290

In this section, we aim to delve into the nuanced advantages and disadvantages of each authentication type. We will elucidate the distinctive traits of knowledge-based, ownership-based, and biometric authentication, highlighting the specific methods falling under each category. Additionally, we will explore the practical considerations and security implications associated with these authentication types, providing a comprehensive understanding of their applications within mobile security frameworks. Figure 1 below shows the conceptual authentication example.

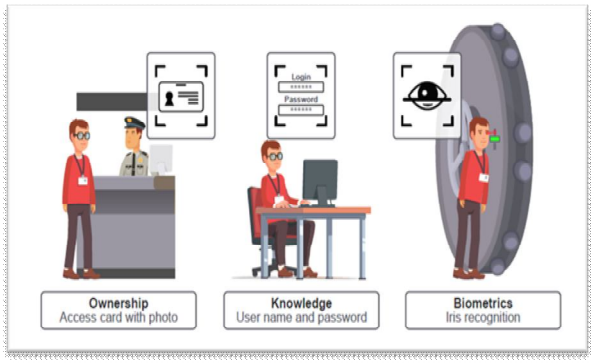

Fig. 1. Conceptual Authentication Example

2.1 Knowledge Based

Knowledge-based authentication relies on information that the user knows [1], typically involving memorized elements like patterns, PINs/passwords, email/password combinations, or security questions. The authentication process typically involves a user entering their email followed by their password. The system then verifies the email's existence and matches the entered password with the stored one. Access is granted upon a successful match, or denied otherwise.

This method's prevalence stems from its ease of use and implementation, contrasting with more complex techniques such as biometric authentication. User convenience holds paramount significance, as an authentication method perceived as inconvenient might dissuade users from returning to the application. Consequently, users tend to create simplistic passwords for ease of memory, often resorting to reusing passwords across multiple platforms. This practice, though convenient, poses substantial risks. If a password is compromised in one place, it potentially jeopardizes security across various sites. Password length significantly influences security, with shorter passwords being more vulnerable to brute-force attacks. For instance, a 4-digit PIN, offering only 10,000 possible combinations, is susceptible to swift brute-force decryption. In contrast, passwords, typically comprising at least six characters incorporating a mix of letters, numbers, and symbols, present a larger possible combination space, enhancing security.

Despite increasing password lengths to deter brute-force attempts, users often craft passwords that remain easily guessable, frequently relying on predictable combinations such as their name or date of birth. Attackers exploit this predictability by targeting specific dictionaries, hastening password decryption. While longer passwords theoretically increase the time required for brute-force attacks, the fundamental issue persists: user-generated passwords often lack the complexity needed to withstand modern hacking techniques. This predicament highlights the necessity for user education on crafting robust, unique, and less predictable passwords to fortify security against evolving cyber threats.

2.2 Biometric

Biometric authentication encompasses two primary categories: physiological and behavioral. Presently, mainstream applications have predominantly embedded physiological biometrics. Physiological authentication relies on unique physical characteristics inherent to individuals, including fingerprints, iris patterns, voiceprints, and facial features [2].

One of the foremost advantages of biometric authentication lies in its user-friendliness. Users can effortlessly access their devices by simply scanning their fingerprints or using facial recognition. Moreover, when optimally implemented, biometric authentication offers a higher level of security compared to several other authentication methods. However, its security efficacy largely hinges on the optimal deployment and environmental conditions. Suboptimal conditions may compromise its security, reducing it to a level akin to knowledge-based authentication [5].

Despite its advantages, each type of biometric authentication presents distinct limitations. For example, facial recognition might falter in low-light environments, impacting its reliability. Similarly, authenticating users based on their voice may prove challenging in noisy surroundings. These limitations underscore the importance of not solely relying on biometric authentication. It's advisable to incorporate backup authentication methods to mitigate the shortcomings of relying solely on biometrics.

The inherent limitations of specific biometric methods necessitate a cautious approach when implementing them. While biometric authentication offers unparalleled convenience and a heightened level of security under optimal conditions, recognizing and addressing these limitations is crucial in designing robust authentication systems. Employing complementary authentication methods alongside biometrics ensures a more reliable and resilient security framework.

2.3 Ownership

Ownership authentication involves verifying users based on possessions they own or possess, such as a debit card or a physical token. In the context of mobile applications, ownership authentication commonly

Volume: 16 Issue: 02 Pages: 6349– 6355 (2024) ISSN: 0975-0290

refers to software token authentication. An exemplary instance is Google Authenticator, a widely utilized ownership authentication method.

In this authentication paradigm, to gain access to an application, users must input a one-time password generated by the service provider. The dynamic nature of these passwords, which change frequently, significantly heightens security by rendering password guessing futile. However, this method typically serves as part of a two-factor authentication system, a concept that will be further explored in this paper.

The implementation of ownership-based authentication usually necessitates either pre-installed software or dedicated hardware to facilitate user verification [6]. Despite the elevated security provided by this method, it's not without drawbacks. One notable limitation involves the user's reliance on carrying a physical object, such as a smartphone or token, consistently. This requirement poses a risk of loss or theft, potentially compromising authentication integrity.

While ownership-based authentication substantially enhances security through its dynamic password generation and verification processes, the inconvenience of relying on physical objects remains a significant consideration. The need for users to constantly carry these objects introduces an element of vulnerability. Balancing the heightened security of ownership authentication with the practicality and potential risks associated with carrying physical objects is pivotal in determining its suitability for specific user scenarios and applications.

III. AUTHENTICATION TECHNIQUES

The authentication landscape comprises three fundamental techniques: Single Factor Authentication (SFA), Two-Factor Authentication (2FA), and Multi-Factor Authentication (MFA). These techniques were developed with a primary focus on bolstering security measures within digital systems and applications.

Single Factor Authentication (SFA) represents the foundational method wherein users validate their identity using a single verification factor, typically a password or personal identification number (PIN). However, as cyber threats evolve, relying solely on SFA for security has proven inadequate, prompting the introduction of more robust methods. Two-Factor Authentication (2FA) emerged as a response to augmenting security measures by requiring users to provide two separate and distinct authentication factors. These may include a combination of something the user knows (like a password) and something the user possesses (such as a one-time code sent to their mobile device). The dual-layered protection significantly fortifies access controls, making unauthorized access more challenging. Multi-Factor Authentication (MFA) takes the concept further by integrating additional layers of authentication beyond two factors. This approach incorporates a broader spectrum of validation methods, potentially combining knowledge-based, possession-based, and biometric authentication elements. MFA's multi-tiered security approach erects formidable barriers against unauthorized access attempts, significantly elevating the overall security posture.

The evolution from Single Factor Authentication to more intricate Multi-Factor Authentication methodologies reflects an industry-wide recognition of the need for heightened security in the face of evolving cyber threats. These progressive authentication techniques strive to create increasingly resilient defense mechanisms against unauthorized access, safeguarding sensitive data and digital identities in an ever-evolving technological landscape.

3.1 Single Factor Authentication (1FA)

Single Factor Authentication (SFA) involves verifying users through a single authentication step, where the traditional email/password combination serves as a prime example. This approach, while user-friendly, hinges solely on a single verification factor, often a password, making it susceptible to vulnerabilities if not fortified adequately. Users tend to create easily memorable passwords for convenience, inadvertently compromising security in the process. Weak passwords, typically simple or commonly used phrases, pose a significant risk as they can be easily guessed or targeted in hacking attempts. The inherent ease of guessing or cracking weak passwords renders SFA vulnerable to brute-force attacks or dictionary-based hacking techniques. While Single Factor Authentication stands out for its simplicity and user-friendliness, its susceptibility to password-related vulnerabilities necessitates caution. Recognizing the potential risks posed by weak passwords is crucial, prompting the need for user education and the adoption of stronger authentication measures to mitigate the inherent vulnerabilities of this authentication type.

3.2 Two-Factor Authentication (2FA)

Two-factor authentication (2FA) represents a two-step user verification process that combines multiple authentication types for heightened security. This method typically involves the combination of different authentication factors. For instance, Google Authenticator often serves as the secondary factor in various applications' authentication processes. In a 2FA scenario, users input their email and password as the initial step, followed by entering a verification code to access their account. Access is granted upon successful completion of both steps; otherwise, access is denied.

For example, the leading online 2FA service such as Duo Mobile App and Google 2-step Verification, either call the enrolled phone for the user’s answer or

Volume: 16 Issue: 02 Pages: 6349– 6355 (2024) ISSN: 0975-0290

send a notification message for the user to approve on the screen to pass the authentication process. Similar authentication methods are also adopted in many other mobile 2FA solutions [10].

The core strength of two-factor authentication lies in its resilience against various attacks. Even if a password is guessed or subjected to brute-force attacks, the additional layer of verification required in 2FA - the second factor - acts as a safeguard. This additional verification factor significantly heightens security, thwarting unauthorized access attempts.

However, it's essential to note that while 2FA offers robust protection against many attack vectors, it may not be impervious to all threats. For instance, in certain scenarios like man-in-the-middle attacks [4], where an attacker intercepts communication between users and the authentication system, 2FA might not provide foolproof defense.

Despite this limitation, two-factor authentication remains a cornerstone in fortifying security measures, significantly enhancing the overall protection of accounts and sensitive information. The incorporation of multiple authentication factors serves as a formidable defense against a wide array of cyber threats, making it an indispensable security measure in today's digital landscape.

3.2 Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) stands as an advanced authentication method mandating users to verify their identity using two or more distinct types of authentication factors [7]. Notably, Two-Factor Authentication (2FA) exists as a subset of MFA, sharing common advantages and disadvantages. The key divergence lies in MFA's greater reliance on biometric authentication as an integral part of the authentication process, distinguishing it from 2FA.

The premise behind MFA rests on the notion that as the number of security factors or layers increases, it significantly heightens the challenge for attackers attempting to breach the system. However, this amplified security stance poses a corresponding challenge for users due to increased complexity [3]. Moreover, the intricacy involved in developing and maintaining such sophisticated systems adds another layer of complexity to MFA implementation.

Consequently, the inception of Multi-Factor Authentication (MFA) aimed to elevate security measures and ensure continuous protection of computing devices and critical services against unauthorized access. MFA expands beyond the two-factor realm by incorporating multiple categories of credentials. Predominantly, MFA emphasizes biometric authentication, leveraging automated recognition of individuals based on their behavioral and biological characteristics.

This heightened security measure requires users to present evidence of their identity through two or more distinct factors, further fortifying security protocols. The evolutionary trajectory of authentication methods, delineating the shift towards MFA, is illustrated in Figure 2.

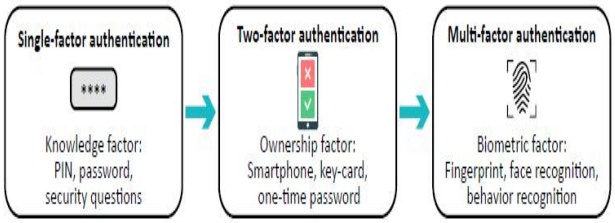

Fig. 2. Evolution of authentication methods from SFA to MFA

IV. PRACTICAL APPLICATIONS OF AUTHENTICATE METHOD IN MODERN SECURITY SYSTEMS

In today's digital age, mobile phones are used for far more than just making calls; they serve as gateways to various services that require high levels of security. For instance, online banking would be significantly less secure if it relied solely on single-factor authentication. This is why Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) have been introduced to verify users before they can access systems and perform online transactions. However, if an application is not user-friendly or easy to register with, users may be deterred from using it again. Given the choice between single-factor and two-factor authentication, users might prefer the simplicity of single-factor authentication, even though it is less secure.

Despite its enhanced security, 2FA often faces usability issues, and relying on passwords alone is inherently insecure. To address these concerns, there is a need for methods that balance usability and security. Passwords and PINs, which are common in single-factor authentication, pose significant risks. Replacing them with alternative authentication factors can mitigate these risks. One proposed solution is password less authentication, where users log in without the need to remember any credentials. Although biometric authentication is a form of password less authentication, it cannot be implemented alone due to its lack of robustness and the high cost of the necessary hardware, such as fingerprint scanners, for laptops and personal computers.

An alternative to the traditional email and password combination is the email-link method, where users log in via a link sent to their registered email address. This method eliminates the need to store or

Volume: 16 Issue: 02 Pages: 6349– 6355 (2024) ISSN: 0975-0290

remember passwords, thereby reducing the risk of password breaches. The security of the email-link method is comparable to the "forgot password" process, where users receive a link with a token to reset their password. The key difference is that the email-link method grants access directly through the link sent to the user's email. By implementing the email-link method, the issue of password management is eliminated, and usability remains comparable to single-factor authentication.

In this paper, we focus on Two-Factor Authentication (2FA) techniques and their applications tested in campus network. Campus networks incorporate security measures such as firewalls, intrusion detection systems, and access control mechanisms. This ensures the protection of sensitive data and personal information, creating a secure digital environment for students and faculty [8]. We explore how 2FA can be tested and implemented in an e-commerce application, allowing users to securely buy and sell items such as books or study materials through the platform using campus network. Additionally, we discuss the feasibility of implementing email-link authentication for users logging in from a web browser, highlighting its potential to enhance security without compromising usability.

4.1 E-Commerce Mobile Application

The mobile app's login process utilizes an email-link authentication method for simplicity and security. Initially, users enter their email in a text field and click the "SEND LINK" button, which triggers an email containing a login link such as in Fig3. Upon clicking this link, users are redirected back to the app, where the "SIGN IN" button becomes enabled. Once users sign in, they gain access to the product dashboard as in Fig 4, the first of five dashboards designed for different purposes: product display, cart management, order tracking, purchase details, and seller activities. These dashboards are efficiently implemented using Recycler View to optimize memory usage.

The e-commerce features include easy navigation through menu-based fragments, enhancing user experience over button-based activity navigation. Buyers can perform actions like viewing product details, making purchases, and updating cart items. Sellers can manage their dashboard, update order statuses, add new products, and view buyer details. The app ensures a seamless experience for both buyers and sellers, allowing efficient navigation and interaction within the application as depict in Fig 5- Fig 9.

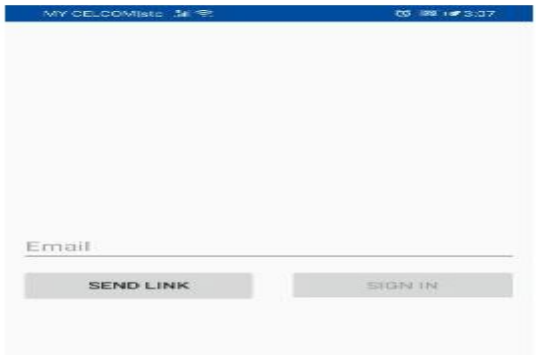

Fig.3 : Login User Interface Prototype

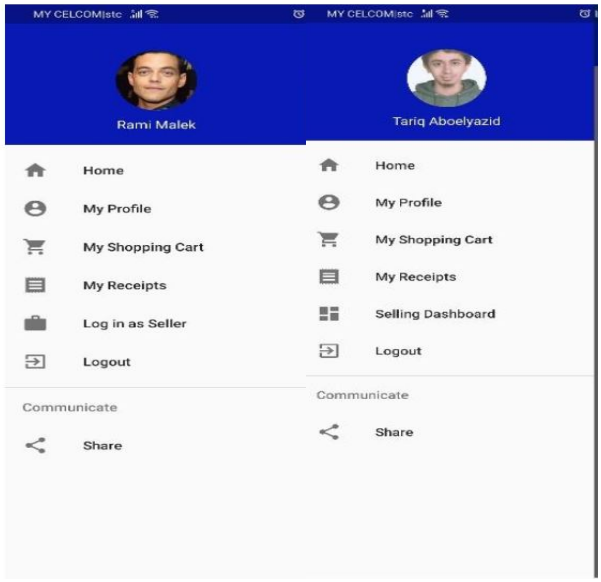

Fig. 4. Navigation UI for buyer and seller

Fig. 5. Purchase dashboard UI for buyer

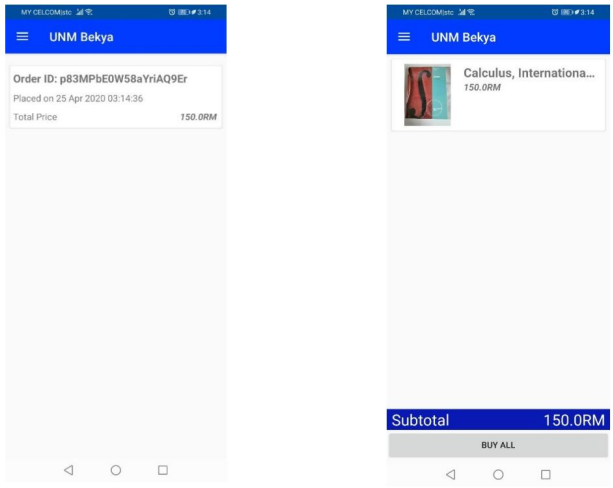

Fig. 6. Order Dashboard UI for Buyer and Cart list UI for Buyer

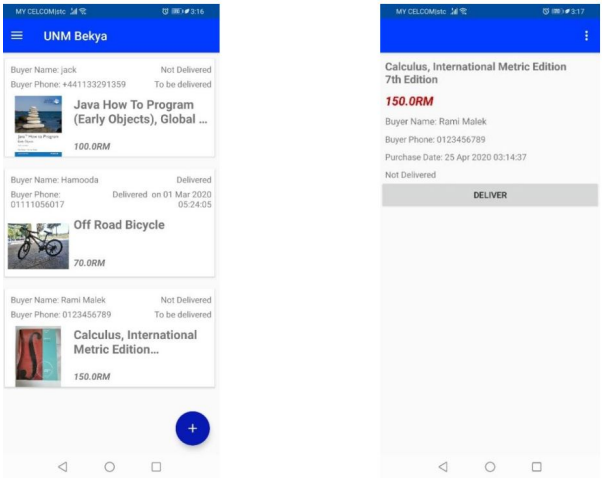

Fig. 7. Seller and buyer dashboard before delivery

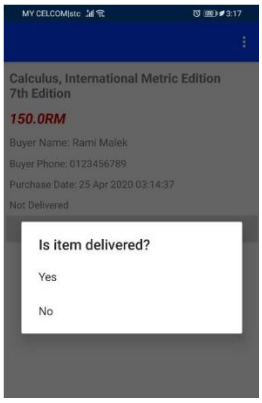

Fig. 8. Delivery Dialog

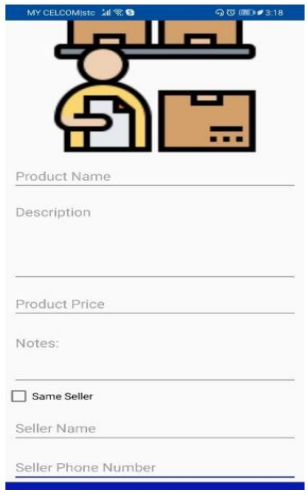

Fig. 9. Add product

4.2 Testing and Feedback on E-Commerce Mobile Application

The feedback collected from a diverse group of students, ranging from Year 1 to PhD, highlighted the importance of user interface and satisfaction with the application design. Most users were satisfied with the design and current features, as indicated by the positive ratings in the survey. Additionally, users expressed a desire for new features, such as the ability to categorize products and edit product details after posting. Despite the simplicity of the application, the majority of users were content with its functionality and design.

In terms of security, around 72% of users felt that the email-link authentication method was secure, although some found it challenging to use in its current implementation. Social login was the preferred authentication method among users, followed by email-link as can see in Fig 12. The feedback suggests that while users appreciate the security provided by the email-link method, there is a need for improvements to enhance its usability and overall user experience depicted in Fig 10 and Fig 11. Time spent on the authentication task is more important for a positive perception of the authentication methods than the objective completion time. Despite the potential time consumption of the 2FA methods, users might be satisfied with the methods in terms of usability and security, especially for highly valued accounts [9].

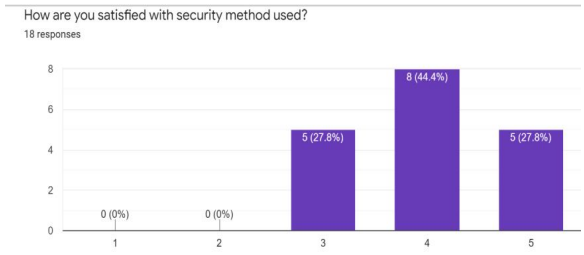

Fig. 10. Survey results on security method

Volume: 16 Issue: 02 Pages: 6349– 6355 (2024) ISSN: 0975-0290

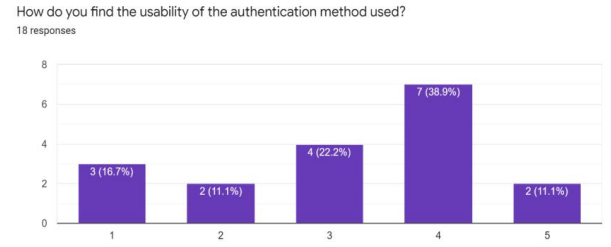

Fig. 11. Survey results on usability

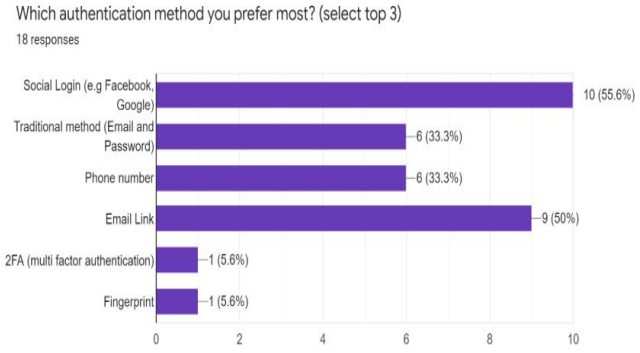

Fig. 12. Survey results on preferred authentication method.

CONCLUSION

The testing of Two-Factor Authentication (2FA) in our sample scenario demonstrated its superior security and user acceptance compared to traditional single-factor methods. Users responded positively to the enhanced security provided by 2FA, highlighting its effectiveness in safeguarding sensitive information. The feedback indicated that, despite some usability challenges, the benefits of 2FA in improving overall security were well-received.

For future work, it is recommended to explore further enhancements to the usability of 2FA, such as simplifying the authentication process and integrating more user-friendly methods. Additionally, investigating the combination of 2FA with emerging technologies like biometric authentication and artificial intelligence could provide even more robust and adaptive security solutions. Continued research into user preferences and behavioral patterns will be essential to refining authentication methods and ensuring they meet both security and convenience needs effectively.

REFERENCES

[1] Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. (2011). On the need for different security methods on mobile phones. Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services - MobileHCI 11 (2011). DOI:http://dx.doi.org/10.1145/2037373.2037442

[2] Syeda Mariam Muzammal, Munam Ali Shah, Si-Jing Zhang, and Hong-Ji Yang. (2016). Conceivable security risks and authentication techniques for smart devices: A comparative evaluation of security practices. International Journal of Automation and Computing 13, 4 (2016), 350–363. DOI:http://dx.doi.org/10.1007/s11633-016-1011-5

[3] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. (2018). Multi-Factor Authentication: A Survey. Cryptography 2, 1 (May 2018), 1. DOI:http://dx.doi.org/10.3390/cryptography2010001

[4] Asoke Nath and Tanushree Mondal. (2016). Issues and challenges in two factor authentication algorithms. Issues and challenges in two factor authentication algorithms 6, 3 (January 2016), 318–327.

[5] Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. (2015. Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. Proceedings 2015 Workshop on Usable Security (2015). DOI:http://dx.doi.org/10.14722/usec.2015.23003

[6] Roland Schlöglhofer and Johannes Sametinger. (2012. Secure and usable authentication on mobile devices. In Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia (MoMM '12), Ismail Khalil (Ed.). ACM, New York, NY, USA, 257-262. DOI=http://dx.doi.org/10.1145/2428955.2429004

[7] Chuck Gehman. What Is MFA (Multi-Factor Authentication)? Retrieved December 2, 2019 from https://www.perforce.com/blog/vcs/what-is-multi-factor-authentication

[8] Alarbad, A.H., Alsharif, A.M. and SatI, S.O. (2024) 'Campus Network Design for Information Technology Faculty', International Journal of Advanced Networking and Applications, 15(06), pp. 6211–6217. doi:10.35444/ijana.2024.15608.

[9] Kruzikova, A., Muzik, M., Knapova, L., Dedkova, L., Smahel, D., & Matyas, V. (2024). Two-factor authentication time: How time-efficiency and time-satisfaction are associated with perceived security and satisfaction. Computers & Security, 138, 103667. https://doi.org/10.1016/j.cose.2023.103667

[10] Ren, Y. et al. (2024) 'Robust Mobile Two-factor authentication leveraging acoustic fingerprinting', IEEE Transactions on Mobile Computing, pp. 1–17. doi:10.1109/tmc.2024.3391184.

BIOGRAPHIES AND PHOTOGRAPHS

Dr Thamilvaani Alvar received the B.Sc. in Computer Science from Coventry University in 2001, the M.Sc. Degree in Software Engineering from Universiti Putra Malaysia (UPM) in 2010, and her Ph.D. in Software Engineering was from UPM too in 2014. She has completed her Post Graduate Certificate in Higher Education (PGCHE) in 2019.She is presently working as an Assistant Professor at the School of Science and Engineering, the University of Nottingham Malaysia. Her research area is mainly Software Engineering, IoT and Cloud Computing.