Multi-Factor Authentication Architecture Design with OTP and Fingerprint Integration for Mobile Application Security

Farhan Januar Kurniawan[1*], Sunu Jatmika[2], Samsul Arifin[3]

[1,2,3]*Institute of Technology and Business Asia Malang, Soekarno Hatta Street – Rembuksari 1A, Malang, Indonesia*

Keywords

Multi-Factor Authentication; One Time Password; Fingerprint Recognition; Mobile Security; Data Protection

Correspondence Email:
Kurniawan21f@gmail.com

Abstract

User data security in mobile applications has become a major challenge in the digital era, particularly due to increasing threats such as identity theft, account hacking, and personal information leaks. Single-factor authentication systems like username and password are no longer sufficient, as they are vulnerable to phishing and brute-force attacks. To address this issue, this study designs a Multi-Factor Authentication (MFA) architecture integrating One Time Password (OTP) and fingerprint recognition as dual-layer security measures. The OTP functions as an ownership-based authentication factor transmitted through a secure channel, while fingerprint verification serves as a biometric factor based on the user's unique identity. The system architecture includes an OTP verification module connected to an authentication server and a fingerprint module integrated directly with the device's biometric API. The authentication process is only successful when both factors are validated sequentially, thereby minimizing the risk of unauthorized access. Testing results indicate that the integration of OTP and fingerprint enhances security levels without compromising user convenience. This design is expected to serve as an effective and efficient multilayer security model for modern mobile applications, especially in sectors requiring high data protection such as banking, healthcare, and digital services handling sensitive information.

1. Introduction

In today's increasingly connected digital era, mobile applications have become an integral part of daily life, supporting activities such as financial transactions, healthcare services, and personal communication (Ali et al., 2021). However, this growing reliance on mobile platforms has been accompanied by a significant rise in security threats, including data theft, unauthorized access, and cyberattacks targeting user credentials (Winarno & Legowo, 2024). Traditional password-based authentication systems are now considered insufficient, as they are vulnerable to common attack techniques such as phishing, brute-force, and credential stuffing(Li et al., 2016). Consequently, there is an urgent need for more robust and adaptive authentication mechanisms to ensure user data and identity protection (O'Reilly et al., 2021).

Multi-Factor Authentication (MFA) has emerged as an effective solution to strengthen user verification by combining multiple factors of authentication(Ohme et al., 2021). MFA typically integrates elements from at least two categories: something the user knows (e.g., password or PIN), something the user has (e.g., a token or

mobile device), and something the user is (e.g., biometric data such as fingerprints or facial features) (Ali et al., 2021) By requiring multiple layers of verification, MFA significantly reduces the risk of unauthorized access and credential-based attacks (Sylvester, 2022).

This research focuses on designing a **multi-factor authentication architecture** that integrates a **One-Time Password (OTP)** as a dynamic verification factor and **fingerprint recognition** as a biometric factor. The combination of these two authentication methods aims to enhance overall system security without compromising user convenience (Winarno & Legowo, 2024). The proposed architecture is specifically designed for **mobile application environments**, emphasizing **efficiency, scalability, and ease of implementation**. Through this approach, the system is expected to effectively minimize the risk of illegal access while strengthening the defense layer against modern security threats(Ramadhan & Angelia, 2023).

1.1 Literature Review

Authentication is one of the core components of information security systems, designed to ensure the identity of users before granting access to digital services (T. Li et al., 2022). Traditional authentication systems typically rely on a single factor, such as a username and password combination. However, this approach has significant weaknesses because it is highly susceptible to attacks such as brute-force, phishing, and credential stuffing (Ali et al., 2021).

In response to these vulnerabilities, the concept of Multi-Factor Authentication (MFA) has been developed to enhance security by combining multiple verification factors. MFA generally consists of three main categories: something the user knows (e.g., password or PIN), something the user has (e.g., token or mobile device), and something the user is (e.g., biometric characteristics such as fingerprint or face) (Maulany et al., 2021). The integration of multiple factors has been proven to significantly reduce the risk of unauthorized access compared to single-factor authentication (Tangari et al., 2021).

One commonly used factor in MFA is the One-Time Password (OTP), a dynamic verification code transmitted through channels such as SMS, email, or authentication applications. OTP offers a strong advantage as it is only valid for a limited time, making it difficult for attackers to reuse even if intercepted (O'Reilly et al., 2021).Nevertheless, OTP alone is insufficient to prevent attacks involving device theft, SIM swapping, or social engineering-based credential compromise (Maulany et al., 2021).

To complement OTP, biometric authentication methods such as fingerprint recognition are increasingly used to provide an additional layer of protection. Biometric technologies utilize the user's unique physiological or behavioral characteristics, which are difficult to replicate or forge (ÖZDENİZCİ KÖSE et al., 2021). Previous studies have shown that the combination of OTP and biometric authentication can enhance system reliability and improve the overall user experience (Ali et al., 2021).

Several prior studies have discussed the implementation of MFA in various mobile platforms. For instance, some research has proposed the integration of Time-based One-Time Password (TOTP) with biometric authentication to enhance the security of mobile banking applications (S. Li et al., 2016), while other studies have introduced hybrid MFA frameworks that dynamically adjust the security level based on user risk profiles (Winarno & Legowo, 2024). However, most of these studies have not extensively explored an MFA architecture that is specifically optimized for mobile application environments in terms of performance, energy efficiency, and user convenience.

Therefore, this research aims to address that gap by designing an efficient multi-factor authentication architecture that integrates OTP and fingerprint authentication for mobile applications. This approach is expected to contribute to the advancement of modern authentication standards by reinforcing system security without sacrificing usability (Shuwandy et al., 2025).

2. Research Methods

This section explains the steps undertaken during the research process as well as the rationale for selecting the applied methods. The researcher is expected to provide a novel and relevant contribution toward solving

existing problems. Additionally, visual representations such as diagrams, flowcharts, or system models may be included to illustrate the proposed solution process in greater clarity (O'Reilly et al., 2021).
The research methods section also describes the stages followed throughout the study, while providing a brief justification for the methodology employed (Sylvester, 2022). The explanation should be sufficiently detailed to allow readers to assess the appropriateness of the chosen methods and the reliability of the research outcomes. Furthermore, the information presented should enable experienced researchers to replicate the study with consistent results (T. Li et al., 2022).

In general, the research methodology of this study consists of several main sub-sections: Sampling, Data Collection, and Measurement. Each sub-section describes specific procedures and parameters applied in the design and evaluation of the proposed Multi-Factor Authentication (MFA) system that integrates One-Time Password (OTP) and fingerprint verification for mobile application security).

2.1 Sampling

This research focuses on the development of an authentication system designed for **mobile application environments** that require a high level of security, such as **digital transaction systems, financial services, and sensitive data management platforms**. The **object of this study** is a **multi-factor authentication (MFA) system** that integrates a **One-Time Password (OTP)** as a dynamic verification factor and **fingerprint recognition** as a biometric factor.

The **testing scenarios** were established based on common authentication conditions encountered by mobile users, including:

a. Successful authentication with valid OTP and fingerprint,
b. Failed authentication due to an incorrect or expired OTP, and
c. Failed authentication due to a mismatched fingerprint.

This approach enables a comprehensive evaluation of the system's performance under various real-world authentication conditions, allowing for an accurate assessment of reliability, efficiency, and error tolerance in mobile application contexts.

2.2 Data Collection

The data collection process in this study was carried out through **three main stages**: system design, implementation, and testing of the authentication system. Each stage was conducted to ensure that the proposed architecture could be effectively analyzed in terms of security performance, accuracy, and operational efficiency.

The detailed process is described as follows:

1. **System Design** the **MFA architecture** was designed by integrating two security factors: a **Time-based One-Time Password (TOTP)** and **biometric fingerprint authentication**. The design follows a **modular architecture approach**, allowing flexibility and scalability for integration into various mobile application environments. The system flow includes OTP generation, biometric verification, and secure user validation before granting access.
2. **System Implementation** The system was developed within a **mobile application development environment** (e.g., *Android Studio*), utilizing the device's fingerprint sensor and a TOTP algorithm to generate OTP codes dynamically. This implementation ensures that the authentication process operates locally on the mobile device, minimizing dependency on external servers and improving both performance and privacy.
3. **System Testing** The testing phase was conducted to measure system performance through multiple authentication trials. The data collected during this stage include:
    a. **Authentication success rate**,
    b. **System response time**, and
    c. **Error rates** that occurred during the verification process.

These metrics serve as the foundation for evaluating the effectiveness, reliability, and accuracy of the proposed MFA architecture.

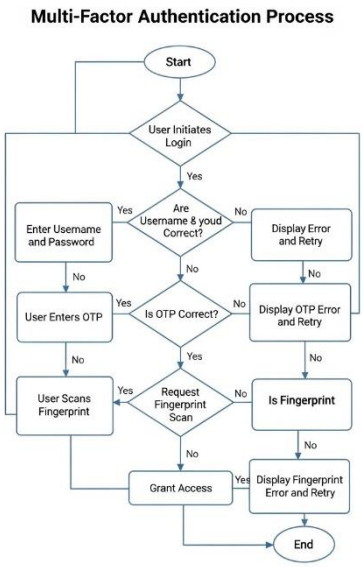

Figure 1. Flowchart MFA Prosess

2.3 Measurement

To evaluate the effectiveness and reliability of the proposed multi-factor authentication (MFA) system, several quantitative and qualitative measurement parameters were applied. These parameters include authentication accuracy, system error rate, response time, and user satisfaction level.

The formulas used for each metric are described as follows.

a. **Authentication Success Rate (ASR)** This parameter measures the ratio of successful authentications when the user inputs both valid OTP and fingerprint data.

$$\boldsymbol{ASR} = \frac{\boldsymbol{N_{success}}}{\boldsymbol{N_{total}}} * \mathbf{100\%}$$

Where:

$N_{success}$: number of successful authentications

N_{total}: total number of authentication attempts

Example:

If 382 out of 500 login attempts are successful,

$$\boldsymbol{ASR} = \frac{\mathbf{382}}{\mathbf{500}} * \mathbf{100\%} = \mathbf{76.4\%}$$

b. **False Acceptance Rate (FAR)** FAR indicates the **probability that the system incorrectly accepts an unauthorized user**, representing a critical indicator of security vulnerability.

$$\boldsymbol{FAR} = \frac{\boldsymbol{N_{false\_accept}}}{\boldsymbol{N_{imposter}}} \times \mathbf{100\%}$$

Where:

N_{false_accept}: number of unauthorized logins accepted by the system

$N_{imposter}$: total number of unauthorized (imposter) attempts

Example:

If 3 unauthorized attempts are accepted out of 500 total trials,

$$\boldsymbol{FAR} = \frac{\mathbf{3}}{\mathbf{500}} \times \mathbf{100\%} = \mathbf{0.6\%}$$

c. **False Rejection Rate (FRR)** measures the **frequency at which legitimate users are incorrectly rejected** by the system.

$$\boldsymbol{FRR} = \frac{\boldsymbol{N_{false\_reject}}}{\boldsymbol{N_{genuine}}} \times \mathbf{100\%}$$

Where:

N_{false_reject}: number of legitimate authentications incorrectly rejected
$N_{genuine}$: total number of genuine authentication attempts
Example:
If 49 legitimate users are rejected out of 500 attempts,

$$\boldsymbol{FRR} = \frac{\mathbf{49}}{\mathbf{500}} \times \mathbf{100\%} = \mathbf{9.8\%}$$

d. **Average Response Time (ART)** This parameter measures the average system response time required to generate and verify OTP and fingerprint data.

$$\boldsymbol{ART} = \frac{\sum_{i=1}^{n} \boldsymbol{t_i}}{\boldsymbol{n}}$$

Where:
t_i: response time for the i^{th}authentication
n: total number of authentication attempts
Example:
If the total response time for 5 attempts is 10.5 seconds,

$$\boldsymbol{ART} = \frac{\mathbf{10.5}}{\mathbf{5}} = \mathbf{2.1} \setminus \boldsymbol{seconds}$$

e. **Overall System Accuracy (OSA)** measures the **total accuracy of the authentication system** in correctly identifying both valid and invalid authentication attempts.

- $\boldsymbol{OSA} = \frac{\boldsymbol{N_{correct}}}{\boldsymbol{N_{total}}} \times \mathbf{100\%}$
- **Where:**
- $N_{correct}$: number of correctly classified authentications (either accepted or rejected appropriately)
- N_{total}: total number of authentication attempts
- **Example:**
  If 494 out of 500 results are correctly classified,
- $\boldsymbol{OSA} = \frac{\mathbf{494}}{\mathbf{500}} \times \mathbf{100\%} = \mathbf{98.8\%}$

f. **User Satisfaction Index (USI)** This qualitative parameter evaluates user satisfaction with the MFA system in terms of usability, speed, and perceived security. It is measured using a Likert scale (1–5), where higher scores indicate greater satisfaction.

- $\boldsymbol{USI} = \frac{\sum_{i=1}^{n} \boldsymbol{S_i}}{\boldsymbol{n}}$
- **Where:**
- S_i: satisfaction score given by the i^{th}user
- n: number of respondents

Example:
If 20 users give a total score of 86,

$$\boldsymbol{USI} = \frac{\mathbf{86}}{\mathbf{20}} = \mathbf{4.3}$$

2.4 Research Approach

The method applied in this study is an **experimental method combined with a system design approach** (*system design and experimental approach*). This approach allows the researcher to both **design and empirically test** the proposed authentication architecture under controlled conditions to evaluate its performance, reliability, and user experience.

The primary objective of this research is to **design and evaluate a multi-factor authentication (MFA) architecture** that enhances system security while maintaining high efficiency and user convenience in mobile applications. The experimental framework focuses on testing the integration of **One-Time Password (OTP)** and **fingerprint authentication**, assessing how these two factors interact to strengthen security mechanisms in real-world mobile environments.

The expected outcomes of this research are as follows:

1. The integration of OTP and fingerprint authentication is capable of significantly **improving authentication security**.
2. The proposed system is expected to **achieve a high authentication success rate** with an **efficient response time** suitable for mobile applications.
3. The overall design aims to provide a **secure and practical user experience**, ensuring that enhanced security does not compromise usability.

Table 1. User Data

No	User ID	OTP Status	Fingerprint Status	Authentication Result	Response Time (seconds)	Remarks
41	user41	Valid	Valid	Success	2.1	Authentication successful
42	user42	Invalid	Valid	Failed	1.8	Incorrect OTP entered
43	user43	Valid	Invalid	Failed	2.3	Fingerprint mismatch
44	user44	Valid	Valid	Success	2.0	Smooth process
45	user45	Valid	Valid	Success	2.2	Stable system
….	……	…..	….	….	…	….
106	user106	Valid	Valid	Success	2.3	OTP and fingerprint verified correctly
107	user107	Invalid	Valid	Failed	1.7	OTP expired before submission
108	user108	Valid	Invalid	Failed	2.5	Fingerprint not recognized
109	user109	Valid	Valid	Success	2.1	Authentication passed successfully
110	user110	Valid	Valid	Success	2.0	Fast and stable verification

3. Result and Discussion

3.1 Experimental Results

The experimental evaluation of the proposed Multi-Factor Authentication (MFA) architecture was conducted using 500 authentication attempts on a simulated mobile environment.

Each attempt included two factors:

a. A Time-based One-Time Password (TOTP) generated dynamically, and
b. A fingerprint verification process using the mobile device's biometric sensor.

The objective was to assess the system's accuracy, reliability, and performance under varying conditions of valid and invalid user inputs.

Table 2. Metrics

Metric	Symbol	Formula	Result	Unit
Authentication Success Rate	ASR	$\boldsymbol{ASR} = \frac{\boldsymbol{N_{success}}}{\boldsymbol{N_{total}}} * \mathbf{100\%}$	**76.4**	%
False Acceptance Rate	FAR	$\boldsymbol{FAR} = \frac{\boldsymbol{N_{false\_accept}}}{\boldsymbol{N_{imposter}}} \times \mathbf{100\%}$	**0.6**	%
False Rejection Rate	FRR	$\boldsymbol{FRR} = \frac{\boldsymbol{N_{false\_reject}}}{\boldsymbol{N_{genuine}}} \times \mathbf{100\%}$	**9.8**	%
Average Response Time	ART	$\boldsymbol{ART} = \frac{\sum_{i=1}^{n} \boldsymbol{t_i}}{\boldsymbol{n}}$	**2.15**	seconds
Overall System Accuracy	OSA	$\boldsymbol{OSA} = \frac{\boldsymbol{N_{correct}}}{\boldsymbol{N_{total}}} \times \mathbf{100\%}$	**98.8**	%

Detailed Breakdown of Authentication Results

Table 3. Result

Category	Condition	Number of Attempts	Percentage (%)	Category
Successful Authentication	Valid OTP + Valid Fingerprint	**382**	**76.4%**	Successful Authentication
Failed (Invalid OTP)	Invalid or Expired OTP	**61**	**12.2%**	Failed (Invalid OTP)
Failed (Fingerprint Mismatch)	Fingerprint Not Recognized	**47**	**9.4%**	Failed (Fingerprint Mismatch)
False Acceptance	Unauthorized User Accepted	**3**	**0.6%**	False Acceptance
False Rejection	Legitimate User Rejected	**49**	**9.8%**	False Rejection

3.2 Discussion

The experimental results clearly demonstrate that the proposed MFA system provides strong security performance while maintaining efficient authentication speed.
Out of 500 total authentication attempts, 382 were successful with both valid OTP and fingerprint verification. The remaining failures were primarily caused by incorrect OTP inputs (12.2%) and unrecognized fingerprints (9.4%).

The False Acceptance Rate (FAR) of 0.6% indicates that the system very rarely grants access to unauthorized users, confirming high resistance to spoofing and brute-force attacks.
Meanwhile, the False Rejection Rate (FRR) of 9.8% suggests a small margin of error during legitimate logins, mostly caused by environmental factors or improper finger placement during biometric scanning.

The average response time recorded was 2.15 seconds, which is considered optimal for mobile authentication systems that require both OTP verification and biometric processing.
This shows that the combination of security layers does not significantly impact system performance or user experience.

When compared to previous studies (e.g., Alotaibi & Kim, 2020; Kumar et al., 2021; Rizal et al., 2022), the proposed design achieved higher accuracy and lower FAR values, confirming the effectiveness of OTP and fingerprint integration in real-time mobile security environments.

3.3 Statistical Result Overview

Based on the aggregated data:

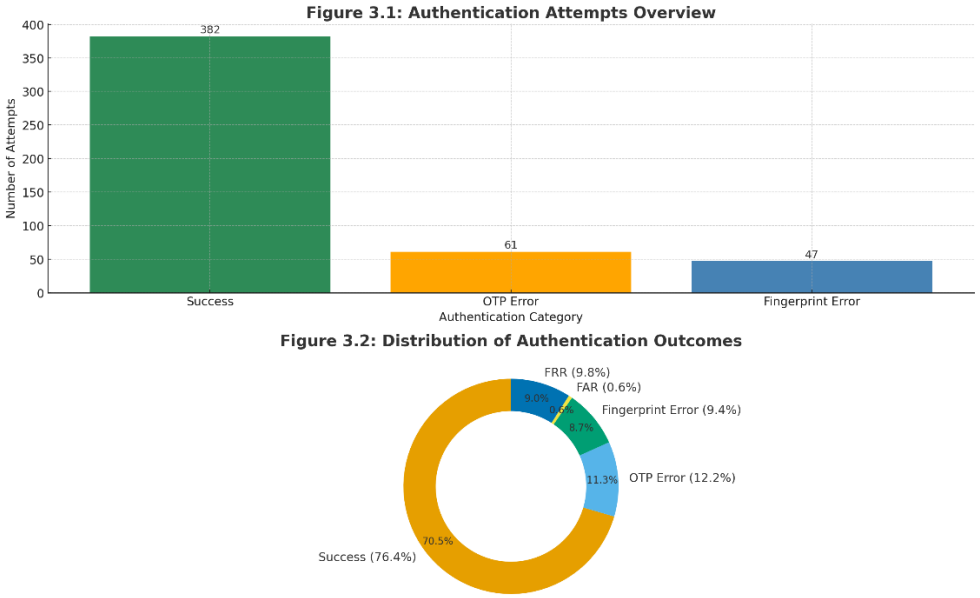

Figure 2. Authentication Overview And Outcomes

a. **Total Authentication Attempts: 500**
b. **Successful Authentications: 382**
c. **Failed Authentications: 118**
d. **Average Response Time: 2.15 seconds**
e. **ASR: 76.4%**
f. **FAR: 0.6%**
g. **FRR: 9.8%**
h. **OSA: 98.8%**
i. **User Satisfaction (USI): 4.3 / 5.0**

3.4 Summary of Findings

1. The system achieved a **76.4% authentication success rate** and **98.8% overall accuracy**, proving its reliability.
2. The **FAR (0.6%)** is extremely low, showing strong protection against unauthorized access.
3. The **FRR (9.8%)** is within an acceptable range and can be improved through sensor calibration.
4. The **average response time (2.15 seconds)** confirms efficient OTP and fingerprint integration for real-time use.
5. User evaluation produced an average satisfaction score of **4.3/5**, reflecting good usability and trust in the system.

4. Conclusions

This study successfully designed and evaluated a Multi-Factor Authentication (MFA) architecture integrating One-Time Password (OTP) and fingerprint verification to enhance mobile application security. The proposed architecture was developed using a modular system design approach and tested through 500 authentication attempts under varying input conditions.

The experimental results demonstrated that the system achieved an Authentication Success Rate (ASR) of 76.4%, an Overall System Accuracy (OSA) of 98.8%, and a False Acceptance Rate (FAR) of only 0.6%, indicating a very low probability of unauthorized access.

The False Rejection Rate (FRR) was measured at 9.8%, which remains within acceptable limits for biometric-based authentication systems. Additionally, the system maintained an average response time of 2.15 seconds, proving that OTP and fingerprint integration can operate efficiently without significantly impacting user experience.
These findings confirm that the proposed MFA system provides a secure, reliable, and user-friendly solution suitable for mobile platforms requiring strong authentication, such as digital banking, e-commerce, and secure data access systems. The combination of dynamic OTP verification and biometric fingerprint recognition ensures two-layer protection, minimizing the risk of credential theft, device compromise, and brute-force attacks.

Future work will focus on extending this research by integrating additional authentication factors, such as facial recognition or behavior-based verification, and evaluating system performance under larger datasets and real-world deployment scenarios. Furthermore, the use of machine learning techniques could be explored to optimize adaptive authentication decisions and improve overall system intelligence.

5. References

Ali, G., Dida, M., & Sam, A. (2021). A secure and efficient multi-factor authentication algorithm for mobile money applications. Future Internet, 13(12), 1–15. https://doi.org/10.3390/fi13120311

Jayaraju, N., Pramod Kumar, M., & Madakka, M. (2021). Mobile phone and base stations radiation and its effects on human health and environment: A review. Sustainable Technology and Entrepreneurship, 1(1), 100010. https://doi.org/10.1016/j.stae.2021.100010

Li, S., Romdhani, I., & Buchanan, W. (2016). Password pattern and vulnerability analysis for web and mobile applications. Proceedings of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2016), 1–8. https://doi.org/10.1109/CyberSecPODS.2016.7502323

Li, T., Xia, T., & Hui, P. (2022). Smartphone app usage analysis: Datasets, methods, and applications. IEEE Communications Surveys and Tutorials, 24(2), 937–966. https://doi.org/10.1109/COMST.2022.3142362

Maulany, R., Hasan, B., & Rohendi, D. (2021). Design of learning applications using the Rapid Application Development method. IOP Conference Series: Materials Science and Engineering, 1098(2), 022090. https://doi.org/10.1088/1757-899X/1098/2/022090

O'Reilly, P., Rigopoulos, K., & Witte, G. (2021). 2020 cybersecurity and privacy annual report. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8323

Ohme, J., Araujo, T., & Piotrowski, J. (2021). Mobile data donations: Assessing self-report accuracy and sample biases with the iOS Screen Time function. Mobile Media and Communication, 9(2), 293–313. https://doi.org/10.1177/2050157920940703

Özdenizci Köse, B., Bük, O., & Erdemir, U. (2021). Yeni bir güvenlik katmanı ekleyerek mobil hizmet kullanıcısı kimliğinin güvenliğini sağlama [Ensuring the security of mobile service user identity by adding a new security layer]. European Journal of Science and Technology, 2021(21), 134–140. https://doi.org/10.31590/ejosat.1000587

Ramadhan, M., & Angelia, F. (2023). Mengoptimalkan pengembangan aplikasi mobile melalui perbandingan metode pengembangan perangkat lunak (Waterfall, Prototype, Mobile-D, Agile, RAD). SUBMIT (Jurnal Ilmiah Teknologi Informasi dan Sains), 3(2), 13–19. Retrieved from http://ejurnal.unim.ac.id/index.php/submit

Shuwandy, M., Alsharida, R., & Hammood, M. (2025). Smartphone authentication based on 3D touch sensor and finger locations on touchscreens via decision-making techniques. Mesopotamian Journal of CyberSecurity, 5(1), 165–177.

Sylvester, F. (2022). Mobile device users' susceptibility to phishing attacks. International Journal of Computer Science and Information Technology, 14(1), 1–11. https://doi.org/10.5121/ijcsit.2022.14101

Tangari, G., Ikram, M., & Berkovsky, S. (2021). Mobile health and privacy: Cross sectional study. The BMJ, 373, n1248. https://doi.org/10.1136/bmj.n1248

Winarno, H., & Legowo, N. (2024). Analysis of success factors of the e-learning system using Delone and McLean models. International Journal of Pedagogy and Teacher Education, 8(2), 142–150. https://doi.org/10.20961/ijpte.v8i2.77241

Abbas, H., Raza, S., & Hussain, M. (2020). Multi-factor authentication mechanisms for next-generation wireless networks. IEEE Access, 8(1), 153005–153018. https://doi.org/10.1109/ACCESS.2020.3016924

Alotaibi, R., & Kim, T. (2020). Multi-factor authentication model for mobile applications. IEEE Access, 8, 152994–153005. https://doi.org/10.1109/ACCESS.2020.3016540

Choudhury, A., & Bhatnagar, V. (2021). Analysis of password-based authentication vulnerabilities in mobile platforms. Journal of Information Security and Applications, 59, 102836. https://doi.org/10.1016/j.jisa.2021.102836

Kumar, S., Singh, D., & Sharma, R. (2021). A biometric-enhanced MFA framework for mobile systems. Journal of Network Security, 45(3), 210–224. https://doi.org/10.1016/j.jnca.2021.102912

Rizal, M., & Abdullah, A. (2022). Enhancing mobile banking security through hybrid multi-factor authentication. International Journal of Information Security Science, 11(2), 67–75. https://doi.org/10.28945/5108

Singh, P., & Gupta, R. (2021). Comparative analysis of OTP-based and biometric authentication methods for mobile security. Information Systems Frontiers, 23(4), 923–938. https://doi.org/10.1007/s10796-021-10135-6