JCTA Journal of Computing Theories and Applications ISSN:3024-9104

Research Article

Mapping Biometric Security Paradox: A Behavioral Study of Perception and Awareness Among Indonesian Digital Natives

Erik Iman Heri Ujianto and Rianto Rianto *

1. Master of Information Technology, University of Technology Yogyakarta, Yogyakarta 55285, Indonesia; e-mail : erik.iman@uty.ac.id
2. Department of Data Science, University of Technology Yogyakarta, Yogyakarta 55285, Indonesia; e-mail : rianto@uty.ac.id

* Corresponding Author : Rianto Rianto

Abstract: The rapid adoption of smartphones among Indonesian digital natives has increased reliance on biometric authentication systems. However, empirical evidence regarding the relationship between user satisfaction and security risk awareness remains limited, particularly in developing-country contexts. This study investigates the behavioral dynamics of biometric security perception among 266 respondents, consisting of 221 high school students and 45 university students in Indonesia. A Python-based computational pipeline incorporating Akaike Information Criterion (AIC) validation and 1,000-iteration stochastic bootstrapping was employed to evaluate nonlinear behavioral patterns using Polynomial Regression and Ordinary Least Squares (OLS) multivariate analysis. The results confirm the existence of a nonlinear Security Paradox. While the overall population demonstrates a positive quadratic trajectory, the university student group exhibits a concave-down parabolic relationship ($a=-0.0460$), indicating a decline in perceived utility beyond a specific security threshold. The identified behavioral breaking point occurs at $X\approx5.45$ (95% CI: 2.99–20.77), suggesting that excessive security hardening may reduce perceived usability and increase cognitive friction. Furthermore, the ablation analysis reveals that security risk awareness ($p<0.001$) is the strongest predictor of user satisfaction, exceeding the influence of daily usage intensity. Segment-level analysis further demonstrates behavioral divergence between respondent groups. High school students exhibit relatively uniform satisfaction toward biometric systems, whereas university students display greater variability and more critical perceptions regarding authentication friction. These findings indicate that highly rigid security configurations may become less effective for users with higher digital literacy and risk awareness. This study contributes a computationally validated behavioral framework for understanding security–utility trade-offs and provides a conceptual foundation for developing adaptive, user-centric, and friction-aware biometric authentication systems..

Keywords: Adaptive Authentication; Behavioral Cybersecurity; Biometric Authentication; Digital Forensics; Digital Natives; Human-Centered Security; Mobile Security; Risk Awareness

Received: March, 31st 2026
Revised: May, 20th 2026
Accepted: May, 21st 2026
Published: May, 27th 2026

1. Introduction

The rapid integration of biometric authentication into mobile devices has transformed personal data security from traditional knowledge-based mechanisms, such as passwords and PINs, toward physiological-based authentication systems [1], [2]. Among the available modalities, fingerprint and facial recognition have become the dominant authentication approaches among Indonesian digital natives due to their balance between usability and perceived reliability [3], [4]. As smartphones increasingly serve as the primary gateway for financial transactions, social communication, academic activities, and other sensitive digital services, the reliability of biometric authentication systems has become an increasingly important concern. Consequently, this study focuses on the security awareness of teenagers and

university students, representing one of the most active demographic groups in smartphone usage, particularly in relation to their dependence on biometric authentication technologies.

The motivation for investigating Indonesian digital natives is closely related to the region's socio-technical characteristics. Despite ranking among the highest globally in smartphone usage intensity, Indonesian youth demonstrate substantial variation in digital privacy literacy and cybersecurity awareness. This imbalance creates conditions in which rapid technological adoption may not always be accompanied by proportional understanding of security risks. In contrast to digitally mature environments where security practices are more systematically institutionalized, Indonesian digital natives often interact with biometric technologies in a rapidly evolving ecosystem where convenience may outweigh critical security consideration. Such conditions suggest that conventional linear behavioral assumptions may be insufficient to fully capture localized patterns of security perception and user adaptation.

Previous studies on biometric security have primarily emphasized technical evaluation metrics, including False Acceptance Rate (FAR) and False Rejection Rate (FRR), to assess authentication performance [5], [6]. Other studies have examined user adoption through established behavioral frameworks such as the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) [7], [8]. Although these approaches provide valuable insights into system performance and technology adoption, they often provide limited discussion regarding the relationship between perceived satisfaction, security awareness, and behavioral adaptation, particularly in developing-country contexts. This limitation is important because user behavior and security negligence remain critical factors affecting the effectiveness of digital security systems [9], [10].

The central issue examined in this study is the "Security Paradox" among young biometric users. In this context, the paradox refers to a condition in which high satisfaction with biometric authentication may coexist with insufficient awareness of potential security vulnerabilities, potentially reducing proactive security behavior. In addition, the increasing reliance on smartphones for sensitive activities raises questions regarding whether current single-modal biometric systems remain sufficient to address evolving user security expectations [11], [12]. To investigate these issues, this study employs a nonlinear quantitative mapping approach based on polynomial regression analysis. Compared with conventional linear alternatives and basic behavioral models, the proposed approach is intended to better capture potential non-monotonic relationships among smartphone usage intensity, user satisfaction, and perceived demand for stronger authentication mechanisms. The modeling process is further supported through Akaike Information Criterion (AIC)- based model comparison and bootstrap validation within a behavioral survey framework.

The main contributions of this study are summarized as follows:

- Nonlinear Behavioral Mapping: Identifying potential curvilinear patterns between smartphone usage intensity and security awareness among Indonesian digital natives.
- Multi-layer Authentication Insight: Examining user tendencies toward multimodal biometric preferences, such as iris or voice recognition, in response to perceived security concerns despite relatively high satisfaction with current systems.
- Behavioral Security Perspective: Providing an exploratory behavioral perspective that may support future studies related to user intent, trust, and non-repudiation in biometric-based digital environments [13].

The remainder of this paper is organized as follows. Section 2 presents the preliminaries and related work concerning biometric authentication, user awareness, and behavioral security perspectives. Section 3 describes the proposed methodology, including data collection procedures, respondent demographics, and analytical methods. Section 4 presents the empirical findings and discusses the observed behavioral patterns related to the identified security paradox. Section 5 compares the findings of this study with existing literature and discusses their broader implications. Finally, Section 6 concludes the paper and outlines several directions for future research.

2. Literature Review

This section presents the theoretical background and related studies concerning the intersection of biometric authentication, user behavior, and security awareness. As biometric technologies become increasingly integrated into daily mobile activities, the relationship

between usability, trust, and perceived security has emerged as an important area of investigation, particularly among younger smartphone users. To establish the context for the present study, this section reviews prior work on mobile biometric security, behavioral security awareness, the emerging concept of the "Security Paradox," and the current research gap within the Indonesian demographic context.

Recent studies have further highlighted the dynamic interaction between digital-native behavior and the integrity of modern security systems. The rapid growth of financial technology adoption among Gen Z populations in Southeast Asia has created a digital ecosystem in which convenience frequently becomes a dominant factor in technology acceptance [14]. Within the Indonesian context, cultural and behavioral factors also influence how users perceive trust in automated authentication systems relative to traditional methods [15]. This tendency may reduce user vigilance toward sophisticated spoofing and social engineering attacks [16], [17]. At the same time, the transition from single-modal to multimodal biometric systems introduces additional cognitive demands that may affect user willingness to adopt more advanced authentication mechanisms [18]. Understanding this balance between convenience, perceived protection, and cognitive burden is important for developing adaptive security strategies that remain usable across different levels of user expertise [19]. In addition, discussions surrounding user intent, accountability, and non-repudiation remain relevant in evaluating the broader implications of biometric authentication systems [20].

2.1. The Evolution of Biometric Security in Mobile Environments

Biometric authentication has evolved from a premium security feature into a widely adopted mechanism for identity verification in smartphones and personal digital devices. Early implementations primarily emphasized hardware reliability and recognition accuracy, whereas recent developments increasingly incorporate machine learning techniques to improve physiological recognition performance [21]. At the same time, mobile authentication systems have gradually shifted from single-modal approaches, such as fingerprint or facial recognition, toward multimodal configurations that combine multiple biometric traits to improve authentication robustness [22].

Despite these advancements, the effectiveness of biometric systems is no longer determined solely by technical performance metrics. In practical mobile environments, user interaction patterns, perceived usability, and authentication friction also influence the overall effectiveness of security deployment. As biometric authentication becomes embedded within everyday digital activities, understanding the behavioral implications of these systems becomes increasingly important alongside conventional technical evaluation.

2.2. Human Factors and Security Awareness Literacy

Security awareness within biometric environments extends beyond the ability to operate authentication technologies. It also includes user understanding of privacy risks, data misuse, spoofing threats, and the behavioral practices required to maintain secure digital interactions. Previous behavioral studies have reported a noticeable gap between technological familiarity and actual security literacy among younger users [23].

This phenomenon is particularly visible among digital natives, who generally demonstrate high confidence in using biometric technologies while possessing varying levels of understanding regarding the associated security implications [24]. Such discrepancies may contribute to increased vulnerability to social engineering attacks, credential misuse, and deceptive authentication scenarios. Consequently, the "human factor" remains a critical component in evaluating the effectiveness of modern biometric security systems.

2.3. The Security Paradox and User Perception

Recent literature has introduced the concept of the "Security Paradox," describing situations in which users report high levels of satisfaction and trust in biometric authentication systems while simultaneously expressing concerns regarding privacy and security vulnerabilities [25]. This paradox suggests that convenience and ease of access may influence perceived trust more strongly than a detailed understanding of technical protection mechanisms. Several studies have also shown that educational background, regional context, and digital literacy significantly affect how users interpret the reliability of biometric systems compared with traditional knowledge-based authentication approaches [26]. In many cases, higher convenience

may unintentionally encourage overreliance on automated systems, potentially reducing proactive security behavior.

Emerging theoretical perspectives further suggest that the relationship between security intensity and user satisfaction may not follow a strictly linear pattern. Increasing authentication complexity can improve perceived protection up to a certain point, after which additional security layers may introduce cognitive burden and usability fatigue. This behavioral tendency has been discussed in relation to "security fatigue," where excessive authentication friction gradually reduces user tolerance toward security procedures. Motivated by these observations, the present study employs nonlinear polynomial modeling to explore potential curvilinear relationships among smartphone usage intensity, user satisfaction, and security awareness. Compared with conventional linear approaches, the adopted framework is intended to provide a more flexible representation of behavioral variation and potential saturation effects within biometric security adoption. Model comparison using AIC and bootstrap analysis is further incorporated to support the stability and interpretability of the observed patterns.

2.4. Research Gaps in the Indonesian Demographic

Although biometric security has been widely studied in global contexts, research focusing on the behavioral security patterns of young users in developing countries, particularly Indonesia, remains relatively limited. Many existing security awareness frameworks are derived from Western or East Asian populations and may not fully capture the socio-cultural characteristics of Indonesian digital natives [27]. In addition, previous studies frequently analyze user awareness, usage behavior, and system satisfaction as isolated variables, providing limited discussion regarding their multivariate interaction within real-world mobile environments. As smartphone dependency continues to increase among Indonesian teenagers and university students, there remains limited empirical evidence explaining how perceived convenience, security awareness, and authentication expectations interact across different levels of digital maturity [28].

To address these limitations, this study investigates the behavioral relationship between smartphone usage intensity, perceived satisfaction, and security awareness among Indonesian digital natives using a multivariate analytical framework. Respondents are categorized into high school and university groups to explore how educational maturity and user experience may influence perceptions of biometric authentication and security friction. In addition, the study introduces the Adaptive Security Governor (ASG) framework as a conceptual design perspective intended to support future discussions on adaptive and behavior-aware authentication strategies. Overall, the reviewed literature suggests that existing biometric adoption models often assume that increased user familiarity naturally leads to improved security behavior. However, behavioral responses toward authentication systems may be more complex, particularly in environments where convenience, trust, and perceived protection interact dynamically. The present study therefore aims to provide an exploratory behavioral mapping of these interactions within the Indonesian digital-native context, while identifying areas where perceived satisfaction and security awareness may not always remain aligned.

3. Proposed Method

This study employs a quantitative survey-based approach to investigate security awareness, user perception, and behavioral responses toward biometric authentication among Indonesian digital natives. The overall methodology is organized into several sequential phases, beginning with theoretical formulation and ending with behavioral interpretation. Figure 1 summarizes the overall research pipeline, including theoretical grounding, variable formulation, instrument development, data acquisition, computational analysis, and behavioral interpretation. The implementation details of each stage are described in the following subsections.

3.1. Theoretical Foundation and Literature-Based Variable Formulation

The initial stage of this study is grounded in the theoretical and empirical findings discussed in Section 2. Existing literature on biometric security, security awareness, human-centered cybersecurity, and behavioral authentication models was used to identify the primary dimensions relevant to this study. Rather than conducting an additional standalone literature survey, this phase focuses on synthesizing the reviewed concepts into measurable behavioral constructs suitable for quantitative analysis. This process establishes the conceptual

foundation for examining the relationship between smartphone usage behavior, perceived security effectiveness, risk awareness, and authentication preferences among Indonesian digital natives.

Figure 1. Overview of the proposed research workflow.

3.2. Variable Identification and Instrument Design

Based on the theoretical synthesis, the study identifies several behavioral dimensions associated with biometric security perception. As summarized in Fig. 1, four primary dimensions are defined for analysis, i.e., usage profile, perceived effectiveness, risk awareness, security demand. These dimensions are used to investigate potential inconsistencies between perceived convenience and security awareness, which form the basis of the proposed "Security Paradox" perspective. The identified constructs were subsequently operationalized into a structured questionnaire consisting of 21 survey items. Prior to large-scale deployment, a pilot validation process was conducted using a small respondent group to evaluate question clarity, readability, and overall instrument consistency.

3.3. Data Collection and Participants

Data collection was conducted using an online questionnaire distributed through purposive sampling to participants matching the target demographic criteria. The study obtained 266 valid responses from Indonesian users actively utilizing mobile biometric authentication systems, particularly fingerprint and facial recognition technologies. The respondent distribution consisted of 221 high school students and 45 university students. This segmentation was intentionally retained to explore potential behavioral differences associated with educational maturity and digital experience levels.

3.4. Computational Analysis and Behavioral Mapping

The analytical stage combines descriptive statistical interpretation with computational modeling to examine behavioral patterns related to biometric security perception. The analysis was conducted using a Python-based computational environment involving the Pandas, SciPy, Scikit-learn, and Statsmodels libraries. To explore potential nonlinear relationships between perceived security demand and user satisfaction, this study employs second-degree Polynomial Regression. The model is intended to capture possible curvilinear tendencies in which increasing security intensity may eventually produce diminishing perceived utility or usability fatigue. The quadratic formulation is expressed as follows:

$$Y = aX^2 + bX + c \tag{1}$$

where Y denotes the user satisfaction index, X represents the security intensity demand, and a corresponds to the quadratic coefficient. A negative coefficient value indicates a potential parabolic tendency associated with the proposed Security Paradox interpretation.

To estimate the approximate turning region of the curve, the parabola vertex is calculated using:

$$x_{\text{threshold}} = -\frac{b}{2a} \tag{2}$$

In this study, the calculated threshold is interpreted as an indicative transition region where additional authentication complexity may begin to reduce perceived convenience rather than increase user confidence. In addition to nonlinear modeling, Ordinary Least Squares (OLS) multivariate regression is employed to evaluate the interaction among several behavioral variables simultaneously. This approach is used to identify which variables contribute more strongly to user satisfaction while controlling for other predictors. The regression model is formulated as:

$$Y = \beta_0 + \beta_1 X_{\text{awareness}} + \beta_2 X_{\text{intensity}} + \beta_3 X_{\text{duration}} + \varepsilon \tag{3}$$

where Y represents the satisfaction score, while the independent variables correspond to awareness level, security intensity demand, and biometric usage duration.

To improve analytical reliability and reduce potential model instability, several validation procedures were incorporated into the computational pipeline:

- Model Comparison using AIC: Linear and second-degree polynomial models were compared to evaluate whether nonlinear modeling provided a more suitable representation of the observed behavioral patterns.
- Bootstrap Resampling: A total of 1,000 bootstrap iterations were performed to estimate coefficient stability and confidence intervals under repeated sampling conditions.
- Multicollinearity Analysis: Variance Inflation Factor (VIF) analysis was conducted to evaluate potential multicollinearity among the independent variables in the OLS model.
- Variable Ablation Analysis: Selected independent variables were systematically removed from the regression model to examine their relative contribution to the observed behavioral outcomes.

Finally, the statistical findings were synthesized into a behavioral interpretation framework that contrasts the response tendencies between high school and university participants. This mapping is intended to provide an exploratory perspective on how perceived convenience, security awareness, and authentication expectations interact across different digital-native segments.

4. Results and Discussion

This section presents the empirical findings obtained from the quantitative evaluation of biometric security perception and user behavior among Indonesian digital natives. The analysis focuses on the interaction between perceived security demand, user satisfaction, and behavioral awareness using survey responses collected from 266 participants. To investigate these relationships, the study combines descriptive statistical analysis, polynomial regression modeling, and multivariate OLS regression within a Python-based analytical environment.

The discussion proceeds from descriptive observations toward a broader interpretation of the identified behavioral patterns. Particular attention is given to the proposed "Security Paradox," referring to the tendency in which increased security requirements may eventually reduce perceived usability and satisfaction. Rather than assuming a strictly linear relationship between security intensity and user experience, this study explores whether the interaction follows a more complex nonlinear trajectory.

4.1. Results

The initial analysis examines the distribution of the User Satisfaction Index (Y) across the two respondent segments: high school students ($n = 221$) and university students ($n = 45$). The segmented analysis reveals noticeable differences in response consistency and behavioral variation between the two groups. The high school segment demonstrates relatively concentrated satisfaction scores with a median centered around 4.0 and limited interquartile dispersion. This pattern suggests that younger respondents generally perceive fingerprint and facial recognition systems as convenient and sufficiently practical for daily usage. In contrast,

the university student segment exhibits a broader distribution with greater variance in satisfaction responses, indicating more heterogeneous perceptions regarding biometric authentication systems.

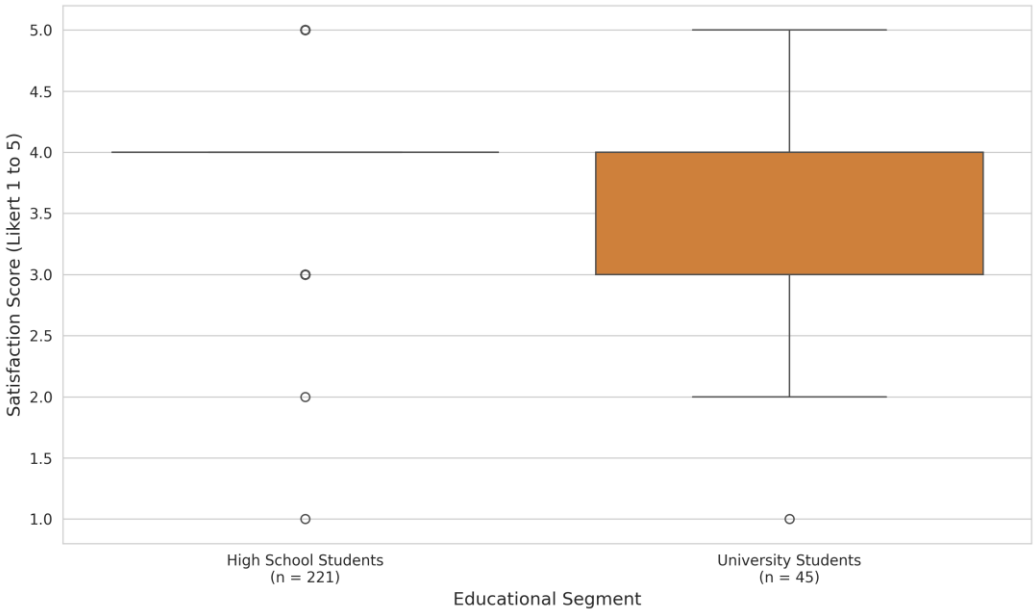

Figure 2. Comparison of User Satisfaction Index (Y) across respondent segments ($N = 266$)

As illustrated in Fig. 2, university students tend to demonstrate more variable evaluations of biometric security systems compared with high school respondents. This broader distribution may reflect increased awareness of security limitations, privacy concerns, or authentication-related usability trade-offs as users gain greater digital maturity and exposure to security-related information.

Building upon this descriptive analysis, the study investigates the proposed "Security Paradox" using second-degree Polynomial Regression within the university student segment. Prior to segment-specific analysis, model comparison was conducted across the full respondent population ($N = 266$) using the AIC to evaluate whether nonlinear modeling provided a more appropriate representation than conventional linear regression.

Table 1. Model comparison based on Akaike Information Criterion (AIC)

Model Architecture	Akaike Information Criterion (AIC)
Simple Linear Regression	579.67
Second-Degree Polynomial Regression	578.39

The polynomial model produced a slightly lower AIC value compared with the linear alternative, suggesting that the nonlinear configuration may better represent the observed behavioral tendencies. The resulting polynomial equation is expressed as:

$$Y = -0.0460X^2 + 0.5014X + 2.3789 \tag{4}$$

where Y represents the user satisfaction index and X denotes the security intensity demand. The negative quadratic coefficient ($a = -0.0460$) indicates a concave-down tendency, suggesting that satisfaction may increase only up to a certain level of perceived security demand before gradually stabilizing or declining.

Using the parabola vertex formulation, the estimated transition region was identified at approximately $X = 5.45$. Bootstrap analysis with 1,000 resampling iterations produced a relatively broad 95% confidence interval ranging from 2.99 to 20.77, indicating that the threshold should be interpreted as an approximate behavioral tendency rather than a fixed deterministic boundary.

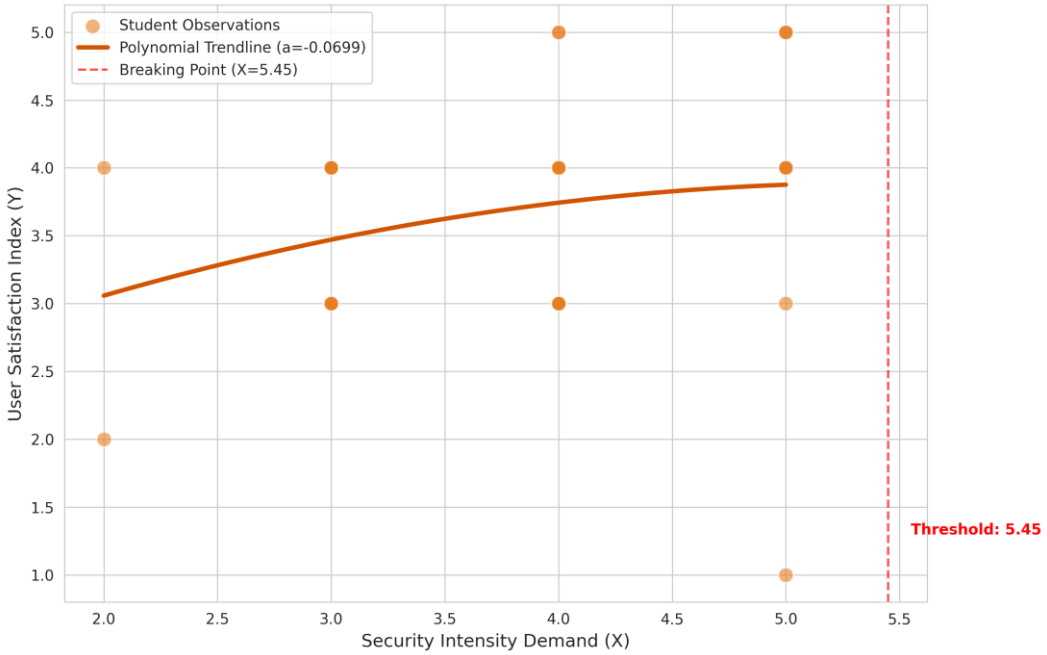

Figure 3. Nonlinear behavioral mapping of the Security Paradox within the university student segment ($n = 45$)

As shown in Fig. 3, the nonlinear curve suggests that increasing security intensity does not necessarily correspond to proportional increases in user satisfaction. Beyond a certain point, additional authentication complexity may introduce usability fatigue or cognitive burden, reducing the perceived convenience of the authentication process. This tendency is consistent with prior discussions regarding security fatigue and authentication friction in human-centered cybersecurity studies.

To further investigate the factors influencing user satisfaction, the study applies OLS multivariate regression incorporating three behavioral predictors: Security Risk Awareness, Daily Usage Duration, and Security Intensity Demand.

Table 2. Multivariate OLS regression analysis for Y

Independent Variable	Coefficient (β)	Std. Error	t-statistic	Variance Inflation Factor (VIF)
Constant	3.2041	0.245	13.078	N/A
Security Risk Awareness	0.3842	0.112	3.430	1.41
Daily Usage Duration	-0.0125	0.025	-0.506	1.07
Security Intensity Demand	0.1458	0.089	1.638	1.48

Note: $*p < 0.05$, $*p < 0.01$. $R^2 = 0.066$; $Adjusted\ R^2 = 0.055$. The dependent variable is the User Satisfaction Index (Y).

The regression analysis indicates that Security Risk Awareness is the strongest predictor within the model, exhibiting a statistically significant positive relationship with user satisfaction ($p = 0.001$). This finding suggests that respondents with higher awareness of digital security risks may evaluate biometric systems more critically while still recognizing their practical value. In contrast, Daily Usage Duration does not demonstrate a statistically significant contribution ($p = 0.613$), indicating that the frequency of smartphone interaction alone may not strongly influence satisfaction toward biometric security systems. Meanwhile, Security Intensity Demand shows a positive but comparatively weaker contribution within the multivariate configuration.

Although the overall explanatory power of the model remains relatively modest ($R^2 = 0.066$), this level is still within a reasonable range for exploratory behavioral studies involving subjective human perception and heterogeneous user backgrounds. The results therefore

should be interpreted as indicative behavioral tendencies rather than deterministic predictive relationships.

To further examine the relative contribution of each variable, a parameter ablation analysis was conducted by systematically removing selected predictors from the regression configuration. The results indicate that removing the Security Risk Awareness variable produces the largest reduction in explanatory performance compared with other variables, reinforcing its importance within the observed behavioral framework. This finding supports the interpretation that perceived security literacy plays a more substantial role in shaping user satisfaction than simple exposure duration or usage frequency. The findings suggest that user responses toward biometric authentication systems are influenced not only by technical convenience but also by varying levels of behavioral awareness and perceived security understanding. These observations highlight the importance of balancing usability and protection mechanisms when designing adaptive biometric authentication systems for digitally active user groups.

4.2. Discussion

The findings of this study indicate that the relationship between biometric security intensity and perceived user satisfaction among Indonesian digital natives is not strictly linear. The observed nonlinear tendency suggests that increasing authentication complexity may initially improve perceived security and trust, but beyond a certain point, additional security mechanisms may introduce usability burden and reduced user comfort. This pattern aligns with broader discussions in human-centered cybersecurity regarding the balance between protection and usability. The polynomial regression results ($a = -0.0460$) suggest the presence of a concave-down behavioral tendency within the university student segment, indicating that satisfaction may gradually stabilize or decline as perceived security intensity increases. Although the estimated transition region was identified around $X = 5.45$, the relatively broad bootstrap confidence interval suggests that this threshold should be interpreted cautiously as an approximate behavioral indication rather than a definitive operational boundary.

Interestingly, the behavioral patterns observed between high school and university respondents demonstrate notable differences in perception consistency. High school respondents generally exhibited more uniform satisfaction scores, suggesting stronger acceptance of existing biometric systems and lower sensitivity toward authentication friction. In contrast, university students demonstrated more heterogeneous responses and greater variability in satisfaction levels. This difference may reflect increased exposure to privacy discussions, digital security awareness, and critical evaluation of authentication systems as educational maturity develops. From a behavioral perspective, these findings may also be associated with the concept of security fatigue, in which increasing verification requirements gradually reduce perceived convenience and user tolerance toward authentication procedures. Rather than viewing stronger authentication solely as an indicator of improved protection, users may simultaneously evaluate the operational effort required to maintain that protection. Consequently, the effectiveness of biometric systems cannot be assessed exclusively through technical robustness but must also consider behavioral sustainability and long-term usability.

The multivariate OLS analysis further reinforces the importance of behavioral awareness within this relationship. Security Risk Awareness emerged as the strongest predictor within the model, suggesting that users with higher awareness of digital threats tend to evaluate biometric systems more critically while remaining conscious of their protective value. In contrast, Daily Usage Duration showed minimal contribution to the observed behavioral outcomes, indicating that frequent interaction with smartphones alone does not necessarily translate into stronger security understanding or higher satisfaction. Although the explanatory power of the regression model remains relatively modest ($R^2 = 0.066$), this outcome is not uncommon in exploratory behavioral studies involving subjective perception and heterogeneous human responses. The results therefore should be interpreted as indicative behavioral trends rather than deterministic predictive conclusions.

The parameter ablation analysis further supports the importance of security awareness within the proposed behavioral framework. Removing the Security Risk Awareness variable produced the largest reduction in explanatory performance compared with the removal of other predictors, indicating that awareness-related factors play a more influential role than simple operational exposure or usage duration.

The observed behavioral patterns suggest that future biometric authentication systems may benefit from adaptive approaches that better balance security mechanisms and usability considerations. In this context, the proposed Adaptive Security Governor (ASG) is introduced as a conceptual design perspective rather than a deployable framework. The concept is intended to encourage future exploration of adaptive authentication strategies capable of responding to varying levels of user awareness, security demand, and behavioral tolerance.

5. Comparison with Existing Studies

The findings of this study complement existing discussions concerning the trade-off between security and usability in biometric authentication systems. Previous studies have generally emphasized either technical performance metrics, such as authentication accuracy and robustness, or broader technology acceptance perspectives using linear behavioral assumptions. In contrast, the present study explores the possibility that user perception toward biometric security may follow a nonlinear behavioral tendency rather than a continuously proportional relationship.

Several conventional adoption models implicitly assume that increasing security measures will consistently improve user trust and perceived safety. However, the behavioral patterns identified in this study suggest that additional authentication complexity may eventually produce diminishing usability benefits, particularly among users with higher levels of security awareness. This observation aligns with prior literature discussing authentication fatigue and cognitive overload in human-centered cybersecurity environments.

Compared with traditional linear approaches, the polynomial regression framework adopted in this study provides a more flexible representation of behavioral variation across different user segments. The analysis indicates that user satisfaction may initially increase alongside perceived security intensity before gradually stabilizing or declining as authentication complexity becomes more intrusive. While this tendency should not be interpreted as a universal behavioral law, it highlights the importance of considering nonlinear user responses in security design evaluation.

The segmentation between high school and university respondents also provides additional behavioral insight. The relatively uniform satisfaction pattern observed among younger respondents contrasts with the more heterogeneous and critical responses demonstrated by university students. This distinction suggests that educational maturity and security literacy may influence how users interpret the balance between convenience and protection. Unlike many existing studies that focus primarily on maximizing authentication robustness, the present work emphasizes the importance of maintaining a balanced interaction between security mechanisms and user experience. Rather than advocating for reduced security, the findings suggest that excessive authentication friction may unintentionally reduce perceived usability and long-term acceptance among digitally active users.

In this context, the proposed Adaptive Security Governor (ASG) is positioned as a conceptual guideline intended to encourage future development of adaptive authentication strategies capable of dynamically balancing security intensity and user convenience. The present study therefore contributes primarily as an exploratory behavioral-computational perspective that complements existing technical and usability-focused biometric security research.

6. Conclusions

This study investigated the relationship between biometric security perception, user satisfaction, and behavioral awareness among Indonesian digital natives using a quantitative behavioral-computational approach. The findings indicate that the interaction between perceived security intensity and user satisfaction may exhibit a nonlinear tendency, particularly among university respondents with higher levels of security awareness. The polynomial regression analysis demonstrated a slightly better empirical fit compared with conventional linear modeling based on Akaike Information Criterion (AIC) evaluation. The observed concave-down tendency suggests that increasing authentication complexity may initially improve perceived protection and trust, but additional security layers may eventually introduce usability burden and reduced satisfaction. The estimated transition region around $X = 5.45$ should be interpreted as an approximate behavioral tendency rather than a fixed operational

threshold, particularly given the relatively broad confidence interval obtained through bootstrap analysis.

The multivariate OLS results further indicate that Security Risk Awareness is more strongly associated with user satisfaction than simple smartphone usage duration. This finding suggests that behavioral literacy and user understanding of digital threats may play a more important role in shaping security perception than exposure frequency alone. Although the overall explanatory power of the model remains limited, the results provide an exploratory indication that behavioral awareness contributes meaningfully to how users evaluate biometric authentication systems. This study also highlights the importance of balancing authentication robustness with long-term usability and cognitive acceptance. Rather than supporting a purely "maximalist" security perspective, the findings suggest that adaptive approaches may be more appropriate for digitally active user populations with varying levels of awareness and behavioral tolerance.

In this context, the proposed Adaptive Security Governor (ASG) is introduced strictly as a conceptual design perspective intended to support future exploration of adaptive authentication strategies. The framework is not presented as a deployable system or finalized technical architecture, but rather as an initial behavioral-oriented guideline for balancing security intensity and user convenience in future biometric environments. Several limitations should also be acknowledged. The study relies on a private survey dataset with a relatively limited respondent distribution, particularly within the university segment. In addition, the behavioral interpretations are based on self-reported perception data and should therefore be interpreted cautiously. Future studies may expand the analysis using larger and more diverse populations, additional public datasets, or longitudinal behavioral observations across different application domains such as mobile banking, financial technology, and digital forensic systems. The results provide an exploratory perspective on the interaction between usability, security awareness, and perceived protection within biometric authentication systems among Indonesian digital natives. The study further suggests that future authentication design may benefit from incorporating behavioral adaptability alongside conventional technical security considerations.

Author Contributions: Conceptualization: E.I.H.U. and R.R.; Methodology: E.I.H.U.; Software: E.I.H.U.; Valida-tion: E.I.H.U. and R.R.; Formal analysis: R.R.; Investigation: E.I.H.U.; Resources: R.R.; Data curation: E.I.H.U.; Writing—original draft preparation: E.I.H.U.; Writing—review and ed-iting: R.R.; Visualization: R.R.; Supervision: R.R.; Project administration: R.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data supporting the findings of this study, comprising anonymized questionnaire re-sponses and statistical analysis, are available from the corresponding author upon reasonable request. The data are not publicly available to protect the privacy and confidentiality of the survey respondents.

Acknowledgments: The authors express their sincere gratitude to the Master of Information Technology (MTI) and Informatics departments at the University of Technology Yogyakarta for their administrative support and laboratory facilities. We are deeply indebted to our colleagues, MTI and Informatics students, and especially to all respondents whose participation was fundamental to this study. Furthermore, the authors acknowledge the use of generative AI tools: Gemini for Python coding assistance, structural organization, and initial drafting, and Grammarly for grammar control and language refinement. However, the authors maintained full supervision over all AI-generated suggestions and assume total responsibility for the technical accuracy and conclusions of this manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] P. Gupta *et al.*, "Biometric Employee Identification Using Mobile Devices: ICT integration of Attendance Monitoring System (AMS) and Human Resource Information System (HRIS)," in *2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, Nov. 2023, pp. 1169–1174. doi: 10.1109/ICAICCIT60255.2023.10465719.

[2] M. Akter *et al.*, "CO-oPS: A Mobile App for Community Oversight of Privacy and Security," in *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing*, Nov. 2022, pp. 179–183. doi: 10.1145/3500868.3559706.
[3] R. Garcia-Martin and R. Sanchez-Reillo, "Vein Biometric Recognition on a Smartphone," *IEEE Access*, vol. 8, pp. 104801–104813, 2020, doi: 10.1109/ACCESS.2020.3000044.
[4] J. Zhang and Y. Wang, "A Survey of Behavioral Biometric Authentication on Smartphones," in *2023 4th International Conference on Machine Learning and Computer Application*, Oct. 2023, pp. 722–729. doi: 10.1145/3650215.3650342.
[5] I. Aphanasyev, A. Bukreev, V. Sitnikov, O. Streltsov, and P. Stupen, "Biometric Venous Verification System for Smartphone," in *2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, Nov. 2022, pp. 1–6. doi: 10.1109/CIEES55704.2022.9990794.
[6] R. Haluška, E. Švenk, M. Pleva, S. Ondás, M.-H. Su, and Y.-F. Liao, "User Recognition in Mobile Applications Using Fingerprint Sensors," in *2023 21st International Conference on Emerging eLearning Technologies and Applications (ICETA)*, Oct. 2023, pp. 171–175. doi: 10.1109/ICETA61311.2023.10344050.
[7] R. Salama *et al.*, "Authentication using Biometric Data from Mobile Cloud Computing in Smart Cities," in *2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)*, Nov. 2023, pp. 445–448. doi: 10.1109/AECE59614.2023.10428426.
[8] A. Patrick, A. Burris, S. Das, and N. Noah, "Understanding User Perspective in a University Setting to Improve Biometric Authentication Adoption," in *Proceedings of the 9th Mexican International Conference on Human-Computer Interaction*, Nov. 2022, pp. 1–10. doi: 10.1145/3565494.3565498.
[9] Y. Yang *et al.*, "Uncovering Security Vulnerabilities in Real-world Implementation and Deployment of 5G Messaging Services," in *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, May 2024, pp. 265–276. doi: 10.1145/3643833.3656131.
[10] M. Wang, K. He, J. Chen, Z. Li, W. Zhao, and R. Du, "Biometrics-Authenticated Key Exchange for Secure Messaging," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2021, pp. 2618–2631. doi: 10.1145/3460120.3484746.
[11] G. Sandeepkumaryadax and S. Loganayagi, "Authenticating Users In Real World Applications using Multi Modal Biometric System For Smartphone's Based Hidden Markov Model Compared With K Nearest Neighbor Algorithm," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Jun. 2024, pp. 1–5. doi: 10.1109/ICCCNT61001.2024.10724975.
[12] S. A. Ali, M. A. Shah, T. A. Javed, S. M. Abdullah, and M. Zafar, "Iris recognition system in smartphones using light version (LV) recognition algorithm," in *2017 23rd International Conference on Automation and Computing (ICAC)*, Sep. 2017, pp. 1–6. doi: 10.23919/IConAC.2017.8082011.
[13] R. Y. Patil and S. R. Devane, "Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 5, pp. 2031–2044, May 2022, doi: 10.1016/j.jksuci.2019.11.016.
[14] R. Iskandar, A. Maksum, and A. Marini, "Digital citizenship literacy in Indonesia: The role of privacy awareness and social campaigns," *Soc. Sci. Humanit. Open*, vol. 12, p. 101697, 2025, doi: 10.1016/j.ssaho.2025.101697.
[15] A. C. M. Lim, L. H. X. Ng, and A. Taeihagh, "Biometric data landscape in Southeast Asia: Challenges and opportunities for effective regulation," *Comput. Law Secur. Rev.*, vol. 56, p. 106095, Apr. 2025, doi: 10.1016/j.clsr.2024.106095.
[16] R. Allafi and A. A. Darem, "Usability and security in online authentication systems," *Int. J. Adv. Appl. Sci.*, vol. 12, no. 6, pp. 1–12, Jun. 2025, doi: 10.21833/ijaas.2025.06.001.
[17] K. Gaur, P. Kumar, S. Tripathi, A. Tyagi, and K. Sharma, "Behavioural Biometrics: A Gait Recognition Approach," in *2025 2nd International Conference on Artificial Intelligence, Metaverse, and Cybersecurity (ICAMAC)*, Oct. 2025, pp. 1–6. doi: 10.1109/ICAMAC67779.2025.11398490.
[18] N. R. Vudathala, "AI-Driven Risk-Adaptive App Architecture: A Dynamic Approach to Authentication and Security in Mobile Applications," *Sarcouncil J. Eng. Comput. Sci.*, vol. 4, no. 7, 2025, doi: 10.5281/zenodo.16225319.
[19] P. Prerna, S. Indora, and D. K. Atal, "Multi-Modal Biometric System: Technological Applications and Future Trends," in *2025 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*, Jun. 2025, pp. 573–583. doi: 10.1109/ICSSAS66150.2025.11080766.
[20] I. Rjab and L. Sliman, "Survey on Biometric Authentication for Decentralized Identity Management: Trends, Challenges, and Future Directions," *Futur. Internet*, vol. 18, no. 3, p. 126, Mar. 2026, doi: 10.3390/fi18030126.
[21] C. Wang, Y. Xiao, X. Gao, L. Li, and J. Wang, "A Framework for Behavioral Biometric Authentication Using Deep Metric Learning on Mobile Devices," *IEEE Trans. Mob. Comput.*, vol. 22, no. 1, pp. 19–36, Jan. 2023, doi: 10.1109/TMC.2021.3072608.
[22] X. X. Zheng, B. Taha, M. M. U. Rahman, M. Masood, D. Hatzinakos, and T. Al-Naffouri, "Multimodal biometric authentication using camera-based PPG and fingerprint fusion," *Pattern Recognit. Lett.*, vol. 197, pp. 1–7, Nov. 2025, doi: 10.1016/j.patrec.2025.06.017.
[23] S. Colabianchi, F. Costantino, F. Nonino, and G. Palombi, "Transforming threats into opportunities: The role of human factors in enhancing cybersecurity," *J. Innov. Knowl.*, vol. 10, no. 3, p. 100695, May 2025, doi: 10.1016/j.jik.2025.100695.
[24] M. S. Hassan, N. H. Mai, N. S. A. Wahab, M. Bin Amin, M. M. Hassan, and J. Oláh, "Decentralized fintech platforms adoption intention in cyber risk environment among GenZ: A dual-method approach using PLS-SEM and necessary condition analysis," *Comput. Hum. Behav. Reports*, vol. 18, p. 100687, May 2025, doi: 10.1016/j.chbr.2025.100687.
[25] I. Ajzen, "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior 1," *J. Appl. Soc. Psychol.*, vol. 32, no. 4, pp. 665–683, Apr. 2002, doi: 10.1111/j.1559-1816.2002.tb00236.x.
[26] A. Sutton and L. Tompson, "Towards a cybersecurity culture-behaviour framework: A rapid evidence review," *Comput. Secur.*, vol. 148, p. 104110, Jan. 2025, doi: 10.1016/j.cose.2024.104110.
[27] H. Zwarts, J. Du Toit, and B. Von Solms, "Towards a Cybersecurity Governance Maturity Model for Critical Infrastructures in Developing Countries," in *Lecture Notes in Networks and Systems*, 2025, pp. 540–553. doi: 10.1007/978-3-031-92605-1_33.

[28] R. A. Rahimi and G. S. Oh, "Beyond theory: a systematic review of strengths and limitations in technology acceptance models through an entrepreneurial lens," *J. Mark. Anal.*, vol. 13, no. 4, pp. 1195–1218, Dec. 2025, doi: 10.1057/s41270-024-00318-x.