Biometric Authentication in Mobile Devices

Pratap Singh Nembang[1], **Dr. Pradeep Karn**[2]
[1]PG Scholar, Lord Buddha Education Foundation, Kathmandu, Nepal
[2]Lecturer, Lord Buddha Education Foundation, Kathmandu, Nepal

Abstract:

As mobile devices become more integrated into our everyday lives, traditional security measures like passwords and PINs are becoming less effective against new security threats. This study examines how effective physiological biometric authentication techniques, such as facial recognition and fingerprint scanning, can be in enhancing mobile security. The research aims to fill existing knowledge gaps by thoroughly evaluating the strengths and weaknesses of different biometric authentication methods. By conducting a detailed analysis of the current literature and critically assessing available biometric technologies, this thesis aims to propose better security protocols for protecting mobile devices. The findings indicate that using biometric authentication can significantly improve device security, making it a strong alternative to traditional security measures. The suggested protocols not only enhance security but also improve the user experience by decreasing reliance on outdated methods.

Key words: *Mobile devices, biometric recognition, fingerprint authentication, authentication methods, device protection.*

1. Introduction

In today's digital age, mobile devices are essential, providing a variety of services ranging from communication to financial transactions. However, this increased usage also brings a greater risk of hacking and unauthorized access. Traditional methods of authentication, like passwords and PINs, are becoming less effective against new security threats. Consequently, there is a growing interest in more secure options, such as physiological biometric authentication. This research looks into how effective physiological biometric methods are on mobile devices and investigates their potential to improve security while ensuring a smooth and user-friendly authentication process (Wang et al., 2020). Physiological biometric authentication uses distinct physical traits—like fingerprints, facial features, and iris patterns—to confirm identity Das et al. (2018). This approach provides a strong mix of enhanced security and user convenience. As continuous authentication methods improve, the use of sensors to track user behavior further minimizes the chances of unauthorized access. In contrast to traditional methods that can be undermined by password sharing or forgetfulness, biometric systems are built to be more dependable and secure. This research examines the increasing significance of biometric authentication in mobile devices and its effect on improving both user experience and security.

2. Problem of Statement

The problem statement emphasizes the growing weaknesses of traditional security methods, such as passwords and PINs, in mobile devices. As technology evolves, these methods are becoming less reliable, highlighting the need for more secure options like physiological biometric authentication (for instance, fingerprint and facial recognition). However, there is a lack of research on how effective continuous physiological biometric authentication is in mobile devices. This study aims to explore the effectiveness of this approach, pinpoint potential challenges and vulnerabilities, and aid in creating a more secure environment for mobile devices. Given the significant role mobile devices play in both personal and professional spheres, improving security features is crucial for safeguarding user data and ensuring a dependable digital experience (Abuhamad et al., 2021).

3. Research Questions

- How does physiological biometric authentication compare to traditional authentication methods in terms of security?
- What are the potential challenges and vulnerabilities associated with physiological biometric authentication?
- How can they be mitigated to develop a more secure mobile device environment?

4. Objectives

- To Implement physiological biometric authentication effectively.
- To Address challenges and weaknesses in mobile authentication devices.
- To Enhance security in biometric authentication.
- To Utilize mobile authentication devices in a corporate attendance system with geolocation tracking.

5. Significance of research

This research project is significant because many people rely heavily on mobile devices, yet ensuring their security remains a major challenge. Traditional security methods, such as passwords, are becoming less effective. The research is exploring a new method known as physiological biometric authentication, which includes techniques like fingerprint recognition and iris or retina scanning. This approach could enhance device security while also being user-friendly. The study aims to evaluate the effectiveness of this method, address any challenges that arise, and contribute to making mobile devices safer for frequent users. This study is deemed particularly important as it tackles a critical issue in mobile device security and seeks to provide valuable insights for both academic research and industry practices. The expected outcomes are likely to inform the development of more secure and user-friendly authentication methods for mobile devices, ultimately improving the overall landscape of cybersecurity.

6. Literature review

The day-to-day dependency on the mobile devices has been resulted in the wider investigation prospects related to the efficient of physiological biometric identification. Enhanced traditional devices have security approach like as PINs and passwords that have taken an important effectiveness focus due to the recent breaches techniques, users ended up provoking mostly due to user convenience-driven behavior that results in frequent password misuse by the user (esp. weak or repeating). Through this type of loophole, sensitive data and personal information’s that have been stored on our mobile devices are at high risk. This Literature explores the advantages and limitations of various biometric approaches, including fingerprint, face, and iris recognition, while addressing issues like false positives, privacy concerns, and the need for robust security protocols. Recent advancements in sensor technology and machine learning are improving biometric accuracy and usability, making these methods more reliable. Additionally, user perception and acceptance of biometrics are key to wider adoption, with cultural and regional factors playing a role in their effectiveness (Wang et al., 2020).

Abuhamad et al. (2021) have carried out an innovative evaluation on field of physiological biometric authentication for the mobile devices, highlighting the behavioral biometrics and the sensor-based techniques. In contrast to more traditional methods, they have highlighted the behavioral fingerprinting' possibility to improve security. The paper examines the advancements and difficulties in the continuous authentication by combining information from the several reliable sources. Particularly, the paper's authors highlight how crucial it is for understanding the user behavior for ensuring a successful implementation (Abuhamad et al., 2021). The increased reliance on mobile devices has raised concerns about the effectiveness of traditional security methods like PINs and passwords, which are often compromised due to user convenience and weak practices (Roy et al., 2017). Mobile devices, now essential for activities like communication and financial transactions, require more secure and convenient authentication methods. This has led to a focus on physiological biometric authentication, such as fingerprints, facial recognition, and iris scans, which offer better security due to their uniqueness and difficulty to replicate.

The study also emphasizes the challenges of traditional authentication methods and how biometrics offer enhanced security by eliminating vulnerabilities associated with passwords and PINs. However, there are still challenges like scalability, integration with various systems, and privacy concerns regarding biometric data usage (Choudhry et al., 2022).. In regions like Nepal, where mobile device usage is growing, implementing biometric authentication can significantly enhance security in IT enterprises by protecting sensitive data and reducing cybersecurity risks.

7. Research Methodology

A research methodology encompasses the techniques, procedures, and strategies for gathering, evaluating, and interpreting data. It is a method or strategy utilized to carry out research. This framework, under which the analysis is conducted, ensures that the study is technically acceptable and employs a coherent strategy to address the research questions or hypotheses. The intended objectives of the study have been satisfied, and the validity and reliability of the research findings are guaranteed by an established research technique.

The chosen research methodology for this research is mixed-method approach that combines both qualitative and quantitative strategies for data collection, evaluation, and interpretation. By employing this methodology, the study ensures the technical soundness and reliability of its findings (Saunders & Thornhill, 201). The research philosophy guiding the study is interpretivism, which emphasizes understanding social processes through qualitative insights. This philosophy supports naturalistic data collection methods, such as interviews and observations, and allows for the analysis of secondary data. The study employs a mixed research design, incorporating semi-structured interviews to gain qualitative insights into user perspectives and quantitative surveys for statistical analysis of the effectiveness of physiological biometric authentication on mobile devices.

To collect and analyze data, tools like Power BI, SPSS, Google Forms, Microsoft Word, and Notepad were used, ensuring accuracy and completeness. The sample included employees from local IT companies, such as Laba and Cube Technologies, selected through non-probability sampling. A total of 520 questionnaires were distributed, with 453 responses received. The study ensures reliability and validity by selecting participants with relevant experience in biometric authentication and using a systematic approach to data analysis. Ethical considerations were carefully addressed to protect participants' rights and security throughout the research process

8. Research Framework

Continuous physiological biometric authentication provides a more reliable and user-friendly alternative to traditional authentication methods, such as passwords and PINs, in mobile devices. By leveraging unique biological traits (e.g., fingerprints, facial recognition, or iris scans), this method minimizes vulnerabilities to unauthorized access, thus enhancing overall security. Additionally, continuous biometric authentication is expected to improve user experience by reducing the need for frequent manual inputs of passwords or PINs, offering a seamless and efficient way to interact with mobile devices. This hypothesis aligns with the study's goals of assessing the efficacy of physiological biometrics compared to traditional authentication methods and addressing potential security concerns inherent in mobile devices.

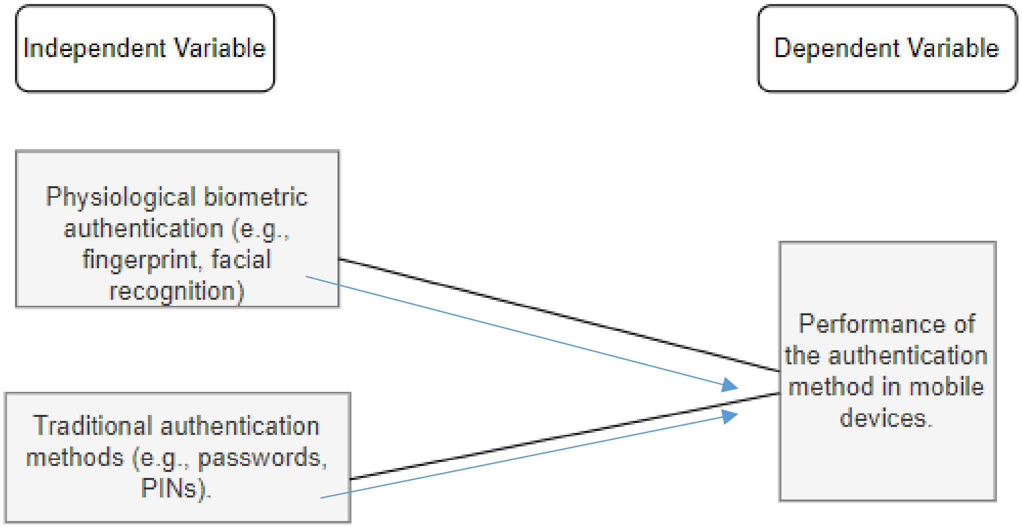

Independent Variable
Dependent Variable
Physiological biometric authentication (e.g., fingerprint, facial recognition)
Traditional authentication methods (e.g., passwords, PINs).
Performance of the authentication method in mobile devices.

Figure 1: Research Framework

The figure presents a research framework that outlines the relationship between independent and dependent variables in the study of mobile device authentication methods. Here's an explanation of the elements:

8.1 Independent Variable

Physiological Biometric Authentication: This represents authentication methods that rely on the user's biological traits, such as fingerprints, facial recognition, and iris scans. These methods are considered more secure and user-friendly as they provide continuous and unique identification without requiring manual input.

Traditional Authentication Methods: These methods involve standard security measures like passwords and PINs, which are widely used but are considered less secure due to vulnerabilities such as weak passwords, reuse across different accounts, and susceptibility to hacking or guessing.

8.2 Dependent Variable

Performance of the Authentication Method in Mobile Devices: The dependent variable represents the outcome being measured in the study. It refers to the effectiveness, reliability, and usability of the authentication methods in mobile devices. The performance includes aspects such as security enhancement, user experience, and protection against unauthorized access.

The above figure illustrates that the study will evaluate the impact of two different independent variables i.e. physiological biometric authentication and traditional authentication methods on the performance of the authentication method in mobile devices. By comparing these methods, the research aims to assess how well they perform in providing secure, reliable, and user-friendly authentication for mobile users.

This framework visually connects the independent variables (authentication methods) with the dependent variable (performance in mobile devices), establishing the basis for the hypothesis and guiding the research methodology.

9. Data analysis

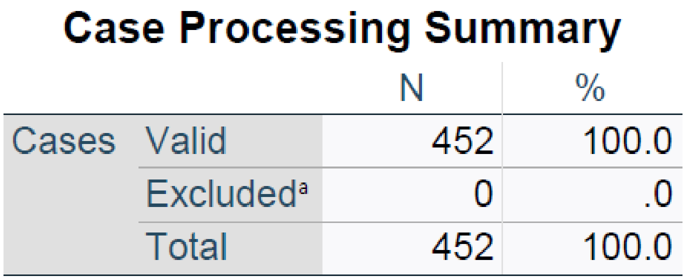
After accomplishing the survey parts, an overview of the data is represented. The processes used for collecting data, filtering data, and analyzing data are all examined well. Through the application SPSS tools, all of the tables and graphs illustrating the statistical results are generated . The goals of the study were mapped into the questions, and in reverse. Therefore, SPSS software was able to load the data with ease, despite the format in which they were gained. This part ensures that the study objectives are satisfied by providing answers to the questions presented in the research question.

9.1 Reliability Testing (Using Cronback's Alpha Reliability Test)

Reliability testing isdone in order to make sure that all the desined questiones listed on the survey assess the exactly the same variables. An effectivenes of biometric authentication in mobile devices can be represented through this survey. For the standard and reliable analysis of data , the survey includes descriptic analysis. The survey questions includes the user beaviour towards the biometric methods in mobile devices. According to the George & Mallery, (2003), below given are the rules made to validate the data analysis:

In terms of quality, 0.9 is considered to be excellent, 0.8 is measured as good, 0.7 is equal to acceptable, 0.6 as questionable, 0.5 is poor and the below 0.5 indicates to be unacceptable.

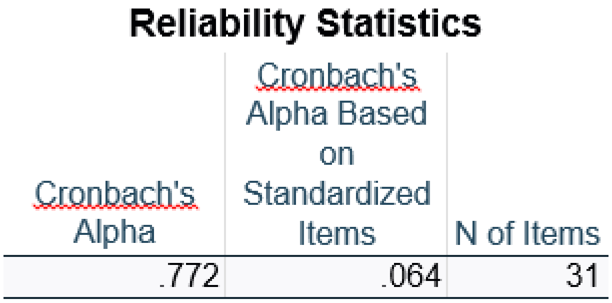
The Cronback's alpha reliability, which ranges from 0 to 1, is employed by SPSS for evaluating reliability. The variables' internal consistency is higher when the coefficient value is nearer 1. The results of Cronback's alpha testing for the survey questions can be seen in the table below. A number of the survey's questions were removed because they didn't really affect the findings.



Case Processing Summary

		N	%
Cases	Valid	452	100.0
	Excluded[a]	0	.0
	Total	452	100.0

Table 1: Case Processing Summary



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.772	.064	31

Table 2: Cronback's Alpha Test

The above shown table, the first table represents the outcomes of the case processing, whereas the second one demonstrates realiability statistics. By employing the George and Malley formula, here we got the coefficient value .772, that means acceptable.

9.2 Demographic Information

Respondent's gender and age groups are categorized and shown in pie chart and barographs.

Participants Gender

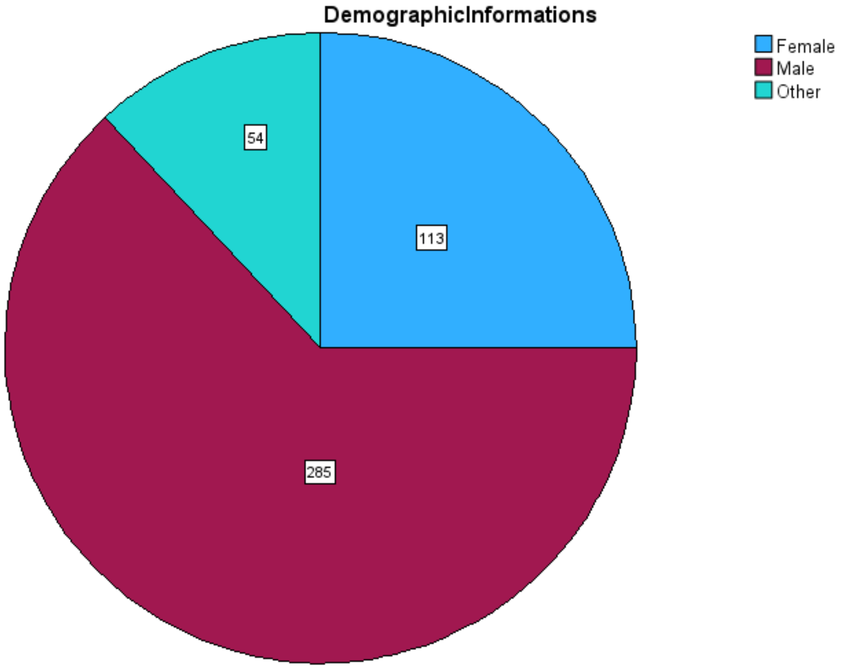


Figure 2: Demonstrations of participants gender information

Gender of Respondents

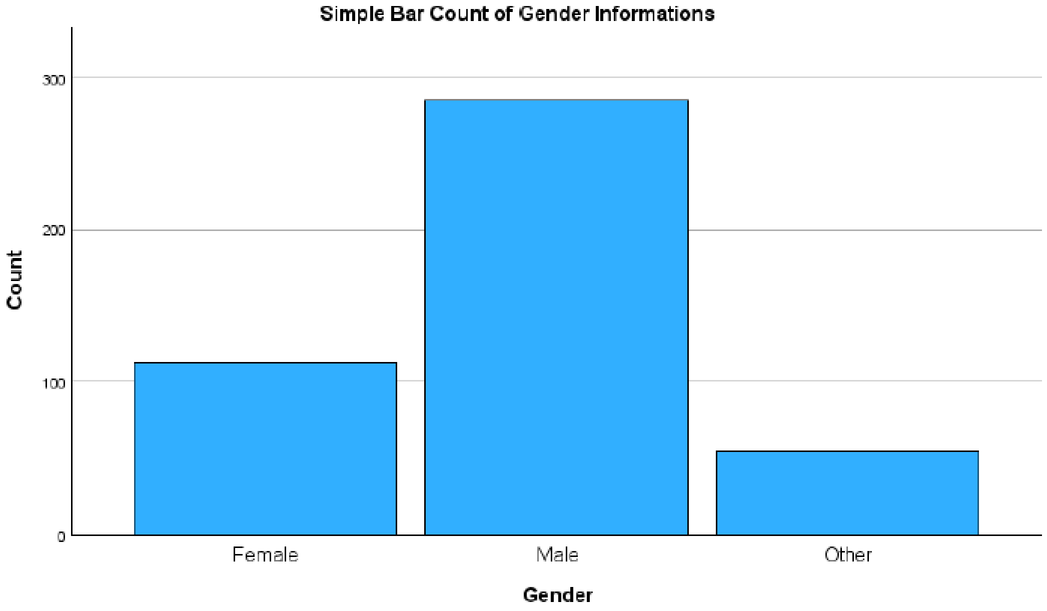
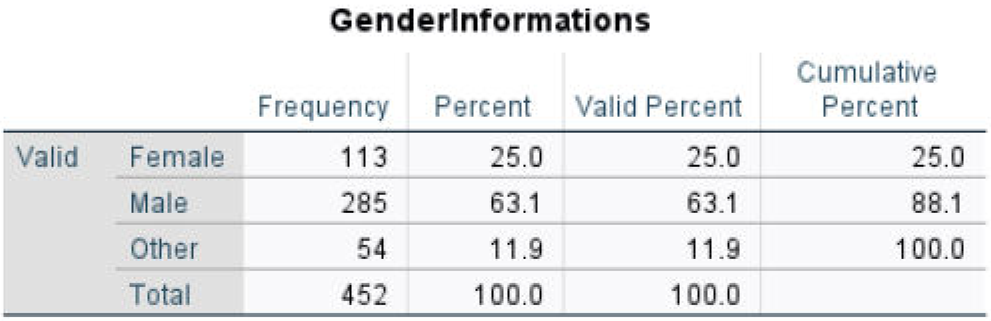


Figure 3: Bargraphs of respondents gender



GenderInformations

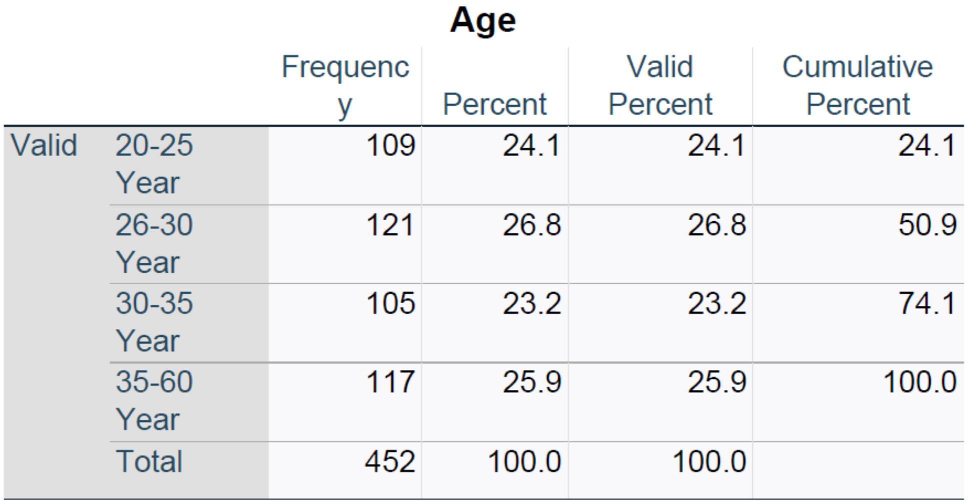
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	113	25.0	25.0	25.0
	Male	285	63.1	63.1	88.1
	Other	54	11.9	11.9	100.0
	Total	452	100.0	100.0	

Figure 4: Table of respondents gender

The research has been carried out interms of gender of the respondents. The above illustrated piechart and bargraphs visualised the males participants were higher in responding the survey. As per the above shown table, there were 452 respondents, of which 25.0 % were female, 63.1 percent were male and the 11.9 % were others.

9.3 Participants Age Group

The survey included the collected data among various age group, which is also an independent variable for the project. The survey respondents discussed the variable biometric authentication, effectivenss and security in other technical ways. We can better understand the efectiveness of the biometric demography by knowing that what age group highly use the authentication approach. People from all age groups are considered to be effective for a data analysis and implementation.



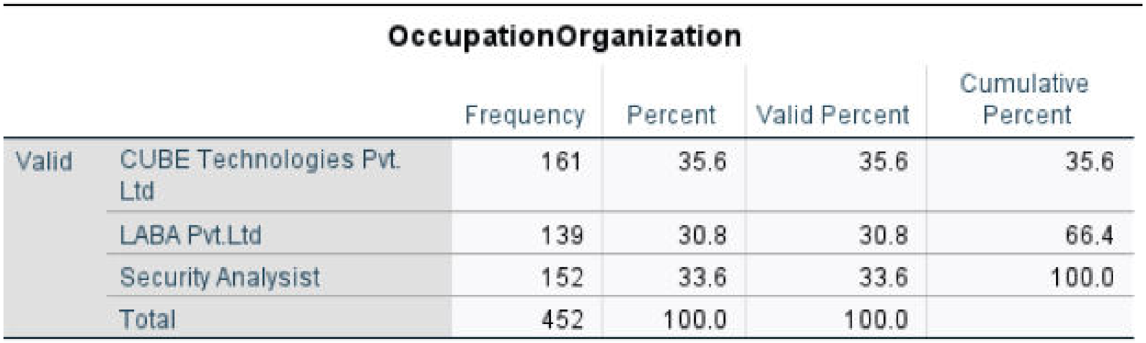
Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20-25 Year	109	24.1	24.1	24.1
	26-30 Year	121	26.8	26.8	50.9
	30-35 Year	105	23.2	23.2	74.1
	35-60 Year	117	25.9	25.9	100.0
	Total	452	100.0	100.0	

Figure 4: Tabular view of respondenst age group

The age group from 26-30 were the higher number of respondents. Young generations are likely to be more keen towards the advancement of new technologies.

9.4 In which organization and occupation are you involved?



OccupationOrganization

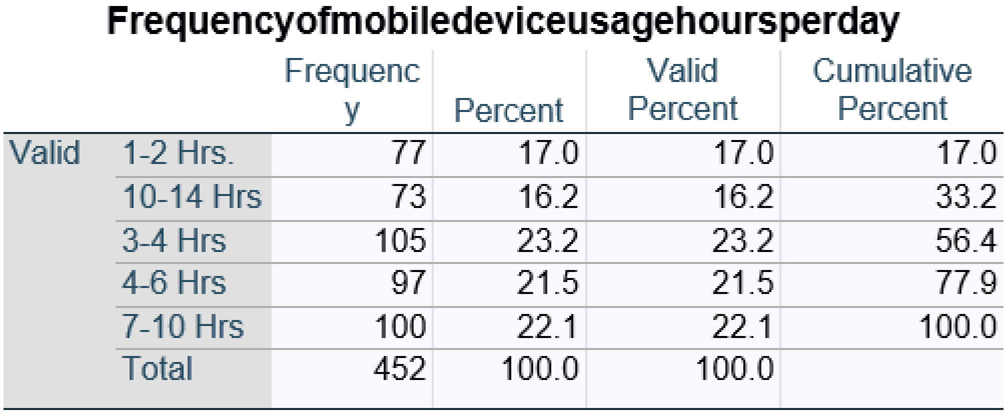
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	CUBE Technologies Pvt. Ltd	161	35.6	35.6	35.6
	LABA Pvt.Ltd	139	30.8	30.8	66.4
	Security Analysist	152	33.6	33.6	100.0
	Total	452	100.0	100.0	

Figure 5: Tabular represntation of participants organizations and occupation

The above table illustrates the breakdowns of respondents based on their occupation or organization, that adds clarity on the participants demographics information in a study on the effectiveness of physiological biometric authentication in mobile devices. CUBE Technologies Pvt. Ltd. comprises 35.6% of the 452 respondents, LABA Pvt. Ltd. for 30.8%, and Security Analysts for 33.6%. There is variety of involvement across these three distinct groups since the overall response rate is 100%. Due to the wide range of professional backgrounds presented in the study, it is possible to improve our understanding of the overall effectiveness of biometric authentication in mobile devices.

9.5 Frequency of mobile device usage hours per day

Understanding respondent's mobile device usage behaviors is important when evaluating the effectiveness of physiological biometric identification, which is why the earlier information analysis may be conducted. Researchers may determine whether there exists a need for safer and more efficient authentication techniques by examining how much time users spend using their devices. Users who use their devices frequently place an emphasis on the simplicity and dependability of biometric solutions. The design and deployment of biometric authentication systems may be supported by this data, assuring that users with different levels of device engagement have their security demands satisfied.



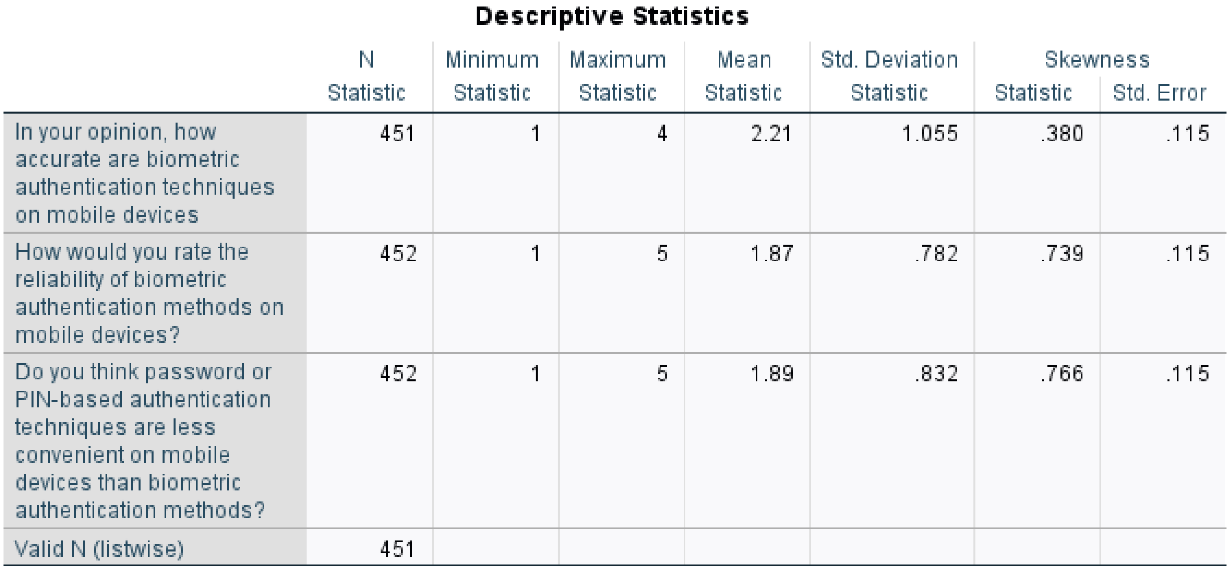
Frequencyofmobiledeviceusagehoursperday

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-2 Hrs.	77	17.0	17.0	17.0
	10-14 Hrs	73	16.2	16.2	33.2
	3-4 Hrs	105	23.2	23.2	56.4
	4-6 Hrs	97	21.5	21.5	77.9
	7-10 Hrs	100	22.1	22.1	100.0
	Total	452	100.0	100.0	

Table 3: Frequency of mobile device usage hours per day

According to the above table, data are divided into the amount of time spent into several ranges, shows statistics on 452 respondents' daily mobile device usage. The highest usage range is between 3 and 4 hours per day (23.2%), with 7 to 10 hours (22.1%) and 4-6 hours (21.5%) following in second and third, respectively. A smaller percentage of participants use their smartphones every day for 10–14 hours (16.2%) or 1-2 hours (17%). In order to assess the effectiveness of physiological biometric authentication, it is fundamental to consider the inequalities in mobile engagement that this distribution highlights. The significance of trustworthy, simple biometric techniques is highlighted by high device usage, especially for users who communicate with the system for a long amount of time.

9.6 Views on Biometric Authentication



Descriptive Statistics

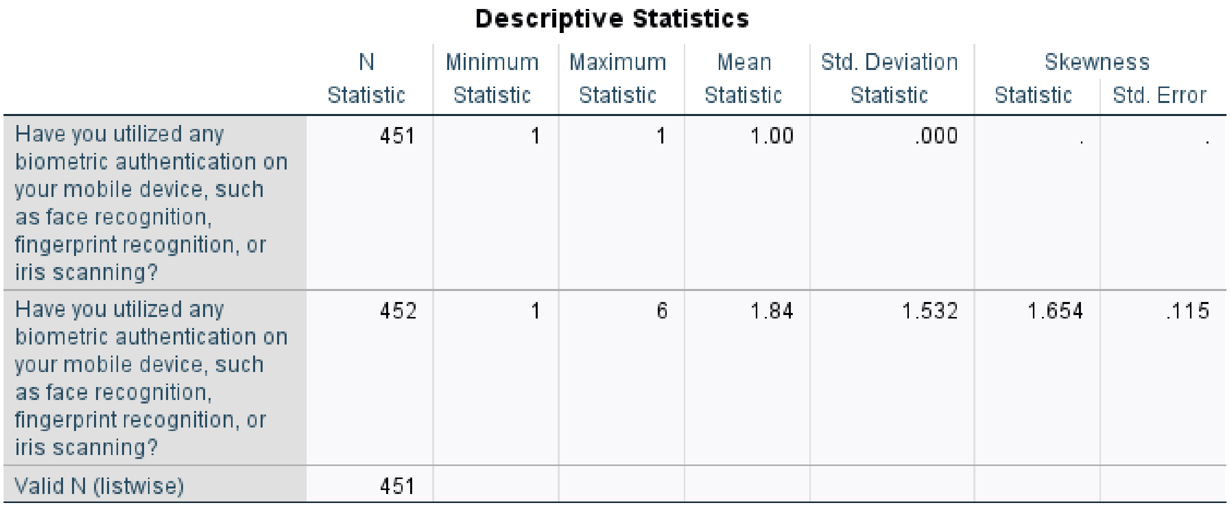
	N	Minimum	Maximum	Mean	Std. Deviation	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
In your opinion, how accurate are biometric authentication techniques on mobile devices	451	1	4	2.21	1.055	.380	.115
How would you rate the reliability of biometric authentication methods on mobile devices?	452	1	5	1.87	.782	.739	.115
Do you think password or PIN-based authentication techniques are less convenient on mobile devices than biometric authentication methods?	452	1	5	1.89	.832	.766	.115
Valid N (listwise)	451						

Table 4: Participants views on Biometric Authentication

The above table provides the descriptive statistics related to the perspectives of the respondents about mobile device biometric authentication. The majority of respondents evaluated accuracy as somewhat, based on the first question's mean score of 2.21 and minor positive skewness of 0.380. The findings of the reliability question indicate that dependability is often less expected than accuracy, with a mean of 1.87 and a skewness of 0.739. In comparison to the first question, the third question, which compares the usefulness of the biometric approach to the password/PIN method, can show that respondents were more likely to agree with the biometric method, with a mean of 1.89 and a skewness of 0.766. There are differing opinions in the data on the viability of biometric authentication.

9.7 Experience with Biometric Authentication

The biometric authentication on mobile devices used by those surveyed are displayed in the table as descriptive data. All 451 respondents seemed to have said "Yes" to employing biometric authentication, based on the first row's mean of 1.00 and lack of variation (standard deviation = 0.00). The second row displays a wider range of answers (mean = 1.84, standard deviation = 1.532), indicating different reactions with various biometric techniques as iris scanning, fingerprint identification, and face recognition. A variety of user experiences and possible variations in the respondents' preferences and effectiveness for different biometric technologies are highlighted by this variability.



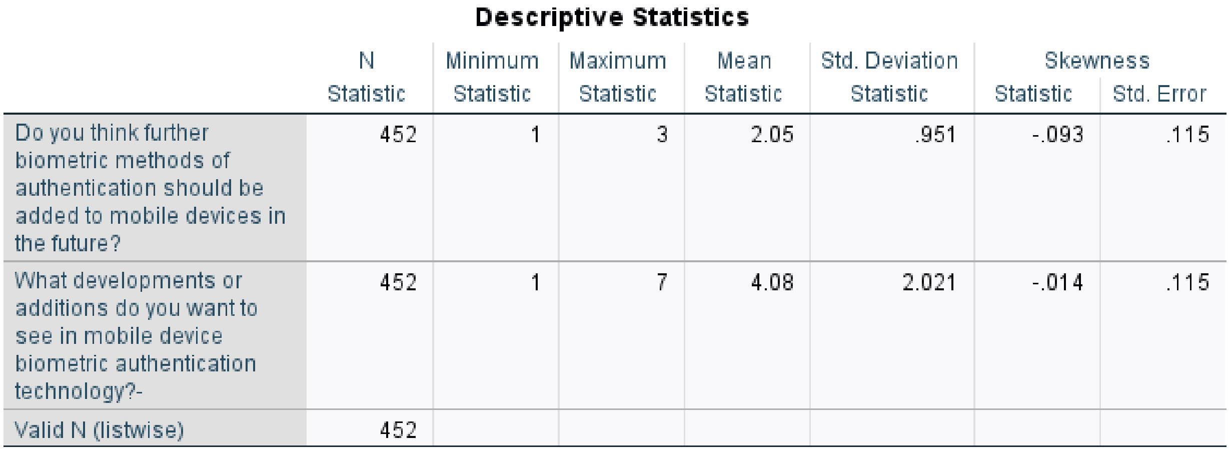
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Have you utilized any biometric authentication on your mobile device, such as face recognition, fingerprint recognition, or iris scanning?	451	1	1	1.00	.000	.	.
Have you utilized any biometric authentication on your mobile device, such as face recognition, fingerprint recognition, or iris scanning?	452	1	6	1.84	1.532	1.654	.115
Valid N (listwise)	451						

Table 5: Tabular illustrating the respondents experience with Biometric Authentication

10. Future Enhancements and Suggestions

The table exhibits statistical information on the respondents' choices for mobile device biometric authentication in the future. The first question on the need of a greater number of diverse biometric means reveals a mean sub-minimum of 2.05 and a weak skewness of -0.093, which marginally refutes the requirement for more ways. The second question, which asked about additions or improvements, had a mean of 4.08, a low skewness value of -0.014, and a high deviation of 2.021. This signifies that cellphones' biometric technology will soon be more advanced and have a greater range of development options. The first two responses offer an appearance of support for system upgrades pertaining to mobile biometric identification.



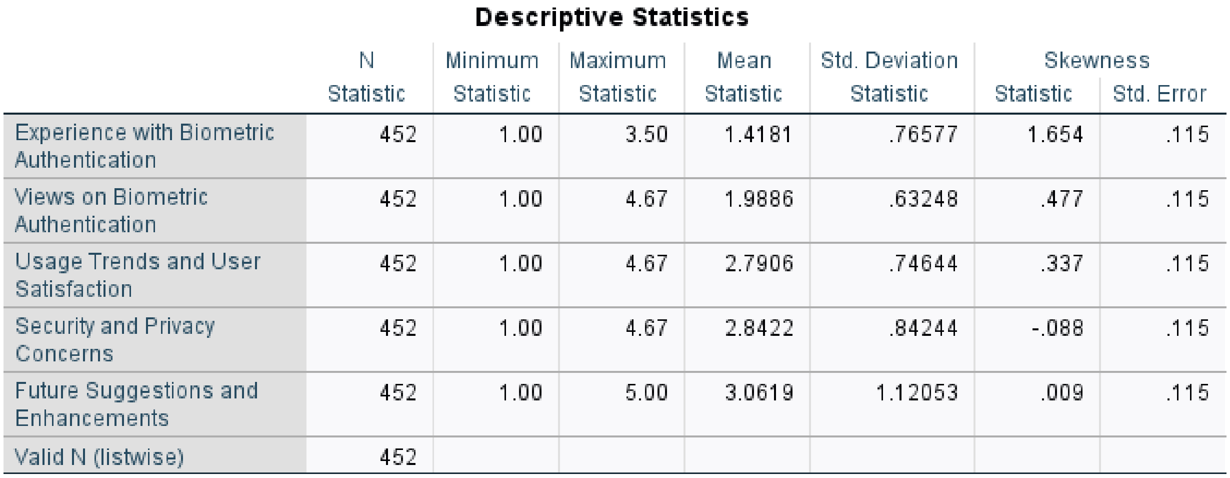
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Do you think further biometric methods of authentication should be added to mobile devices in the future?	452	1	3	2.05	.951	-.093	.115
What developments or additions do you want to see in mobile device biometric authentication technology?-	452	1	7	4.08	2.021	-.014	.115
Valid N (listwise)	452						

Table: Descriptive analysis on future Enhancements and Suggestions

Various aspects related to the effectiveness of physiological biometric authentication

The table provides descriptive data, based on replies from 452 participants, for multiple factors related to the effectiveness of physiological biometric authentication in mobile devices. The medians indicate that, on the whole, respondents are not very satisfied with use trends (mean = 2.7906), have not had much experience with biometric authentication (mean = 1.4181), and are only somewhat concerned about security and privacy (mean = 2.8422). Additionally, attitudes on biometric authentication trend almost in favor (mean = 1.9886). The standard deviations illustrate varying levels of agreement, especially in regards to regard to predictions and improvements for the future (mean = 3.0619, SD = 1.12053), demonstrating different viewpoints about the further development of biometric systems in the future.



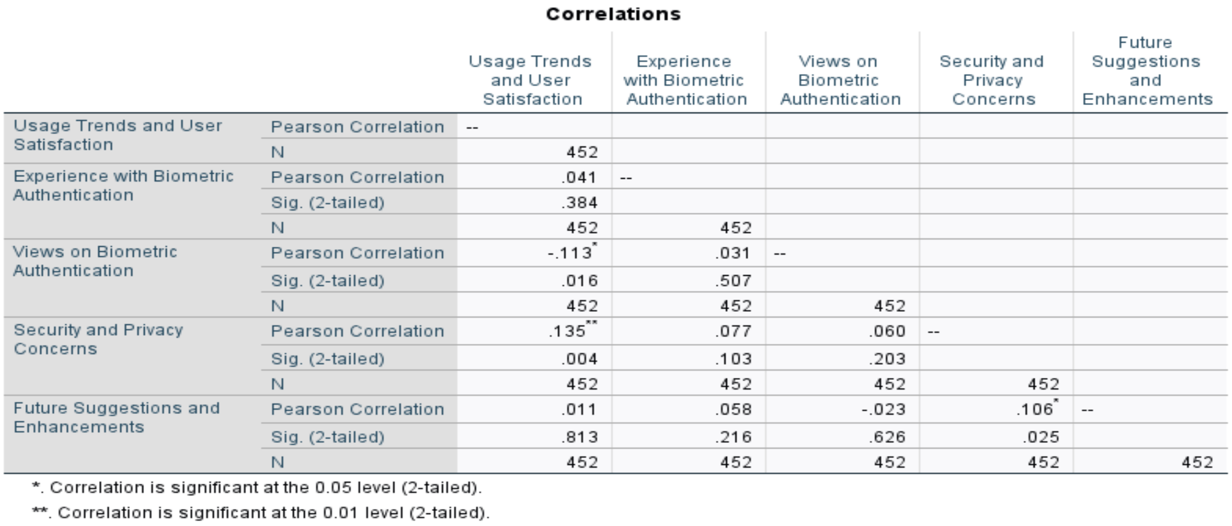
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Experience with Biometric Authentication	452	1.00	3.50	1.4181	.76577	1.654	.115
Views on Biometric Authentication	452	1.00	4.67	1.9886	.63248	.477	.115
Usage Trends and User Satisfaction	452	1.00	4.67	2.7906	.74644	.337	.115
Security and Privacy Concerns	452	1.00	4.67	2.8422	.84244	-.088	.115
Future Suggestions and Enhancements	452	1.00	5.00	3.0619	1.12053	.009	.115
Valid N (listwise)	452						

Table: Summary of Evaluation of the concept

11. Correlation analysis

The correlation matrix analyses the connections among the various factors that involve mobile device physiological biometric identification. Among the notable findings is the positive correlation (r =.135, significant at 0.01) between Security and Privacy Concerns and Usage Trends and User Satisfaction, denoting users who place a higher priority on security can be more satisfied with biometric authentication. The relationship between user satisfaction and views on biometric authentication is negatively correlated (r = -.113, significant at 0.05), suggesting that negative assessments of biometric systems might lower satisfaction with them or utilization.



Correlations

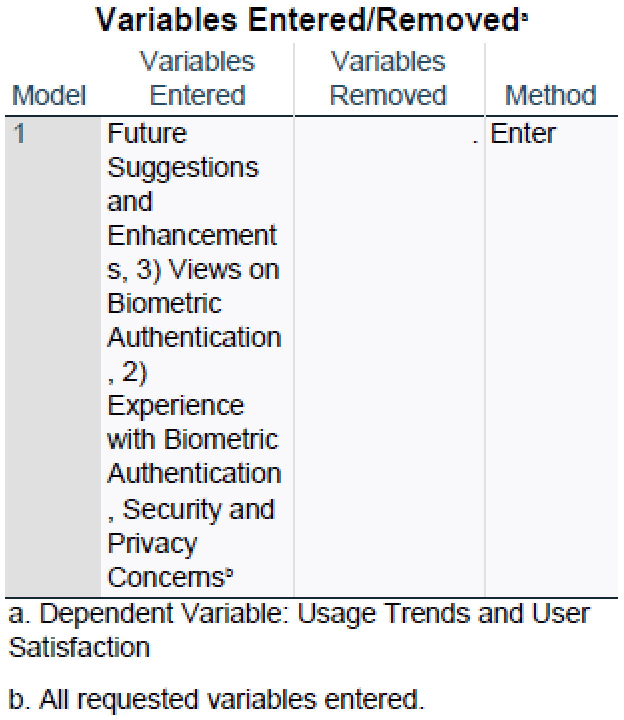
		Usage Trends and User Satisfaction	Experience with Biometric Authentication	Views on Biometric Authentication	Security and Privacy Concerns	Future Suggestions and Enhancements
Usage Trends and User Satisfaction	Pearson Correlation	--				
	N	452				
Experience with Biometric Authentication	Pearson Correlation	.041	--			
	Sig. (2-tailed)	.384				
	N	452	452			
Views on Biometric Authentication	Pearson Correlation	-.113*	.031	--		
	Sig. (2-tailed)	.016	.507			
	N	452	452	452		
Security and Privacy Concerns	Pearson Correlation	.135**	.077	.060	--	
	Sig. (2-tailed)	.004	.103	.203		
	N	452	452	452	452	
Future Suggestions and Enhancements	Pearson Correlation	.011	.058	-.023	.106*	--
	Sig. (2-tailed)	.813	.216	.626	.025	
	N	452	452	452	452	452

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table: Correlation matrix analyses

Regression Analysis:



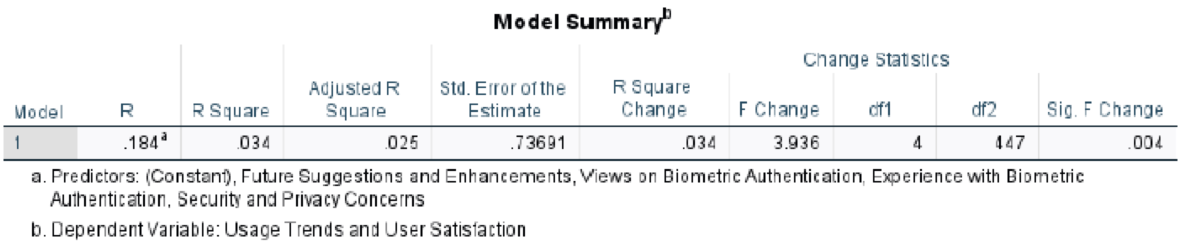
Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Future Suggestions and Enhancements, 3) Views on Biometric Authentication, 2) Experience with Biometric Authentication, Security and Privacy Concerns[b]	.	Enter

a. Dependent Variable: Usage Trends and User Satisfaction

b. All requested variables entered.

Table: Variables Entered



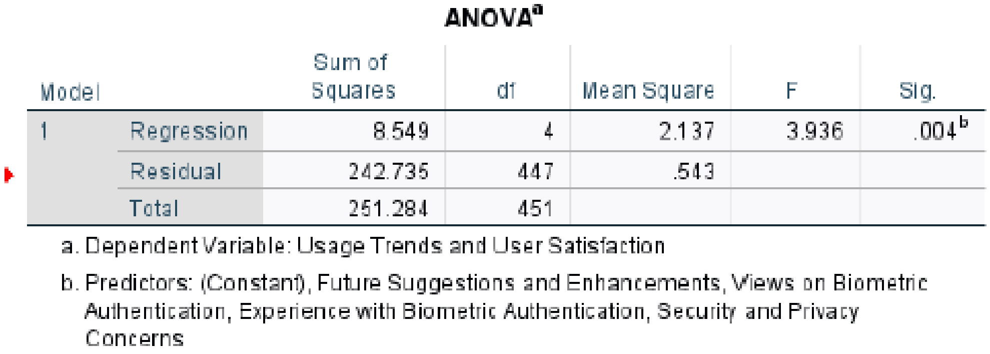
Model Summary[b]

					Change Statistics				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1	.184[a]	.034	.025	.73691	.034	3.936	4	447	.004

a. Predictors: (Constant), Future Suggestions and Enhancements, Views on Biometric Authentication, Experience with Biometric Authentication, Security and Privacy Concerns

b. Dependent Variable: Usage Trends and User Satisfaction

Table: Model Summary



ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8.549	4	2.137	3.936	.004[b]
	Residual	242.735	447	.543		
	Total	251.284	451			

a. Dependent Variable: Usage Trends and User Satisfaction

b. Predictors: (Constant), Future Suggestions and Enhancements, Views on Biometric Authentication, Experience with Biometric Authentication, Security and Privacy Concerns

Table: Anova

12. Conclusions

The study on the effectiveness of physiological biometric authentication in mobile devices compared to traditional methods like passwords and PINs revealed significant insights into its benefits for security and user convenience. Findings from data analysis showed that physiological biometrics, such as fingerprint, facial recognition, and iris scans, offer improved security and are easier to use, with survey respondents reporting higher satisfaction. Reliability testing validated the effectiveness of the survey, with a Cronbach's alpha of 0.772, and demographic analysis ensured the results were applicable across diverse populations and environments. Despite challenges like privacy concerns and the need for ongoing technological advancements to address new security threats, physiological biometrics emerged as a more secure and user-friendly alternative. The study highlights the need for further research on improving biometric technologies and integrating them into existing security protocols while addressing identified limitations. Future research should focus on mitigating these issues and ensuring biometric authentication remains adaptable to emerging threats.

13. References

Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2021). Sensor-based continuous authentication of smartphones’ users using behavioral biometrics: A contemporary survey. IEEE Internet of Things Journal, 8(1), 65–84. https://doi.org/10.1109/jiot.2020.3020076

Akhtar, Z., Micheloni, C., & Foresti, G. L. (2015). Biometric Liveness Detection: Challenges and Research Opportunities. *IEEE Security & Privacy*, *13*(5), 63–72. https://doi.org/10.1109/msp.2015.116

Choudhry, M. S., Pankhil, Nikhurpa, P. S., & Verma, P. K. (2022). A review on physiological attributes based biometric authentication. 2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS). https://doi.org/10.1109/ic3sis54991.2022.9885495

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones–A survey of attitudes and practices. Computers & Security, 24(7), 519-527.

Das, A., Galdi, C., Han, H., Ramachandra, R., Dugelay, J.-L., & Dantcheva, A. (2018). Recent advances in biometric technology for mobile devices. *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. https://doi.org/10.1109/btas.2018.8698587

Dharavath, K., Talukdar, F. A., & Laskar, R. H. (2013). Study on biometric authentication systems, challenges and future trends: A Review. 2013 IEEE International Conference on Computational Intelligence and Computing Research. https://doi.org/10.1109/iccic.2013.6724278

Farzin, H., Abrishami-Moghaddam, H., & Moin, M.-S. (2008). A Novel Retinal Identification System. *EURASIP Journal on Advances in Signal Processing*, *2008* (1).

Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric Antispoofing Methods: A Survey in Face Recognition. *IEEE Access*, *2*, 1530–1552. https://doi.org/10.1109/ACCESS.2014.2381273

George, D., & Mallery, P. (2003). SPSS for Windows Step by Step. Allyn & Bacon.

Hu, M., Zhang, K., You, R., & Tu, B. (2023). Multisensor-based continuous authentication of smartphone users with two-stage feature extraction. *IEEE Internet of Things Journal*, *10*(6), 4708–4724. https://doi.org/10.1109/jiot.2022.3219135

Jain, A. K., Lin Hong, Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, *85*(9), 1365–1388. https://doi.org/10.1109/5.628674

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, *43*(2), 90–98. https://doi.org/10.1145/328236.328110

Keng Lin Soh, Wai Peng Wong, & Kok Leong Chan. (2010). Adoption of Biometric Technology in Online Applications. *The International Journal of Business & Management*, *3*(2), 121.

Koong, C.-S., Yang, T.-I., & Tseng, C.-C. (2014). A user authentication scheme using physiological and behavioral biometrics for multitouch devices. *The Scientific World Journal*, *2014*, 1–12. https://doi.org/10.1155/2014/781234

L Karthik Narayan, Sonu. G, & Soukhya S. M. (2020). Fingerprint Recognition and its Advanced Features. *International Journal of Engineering Research And*, *V9*(04). https://doi.org/10.17577/ijertv9is040393

Laux, D., Luse, A., Mennecke, B., & Townsend, A. M. (2011). Adoption of Biometric Authentication Systems: Implications for Research and Practice in the Deployment of End-User Security Systems. *Journal of Organizational Computing and Electronic Commerce*, *21*(3), 221–245. https://doi.org/10.1080/10919392.2011.590111

Li, L., Mu, X., Li, S., & Peng, H. (2020). A Review of Face Recognition Technology. *IEEE Access*, *8*, 139110–139120. https://doi.org/10.1109/access.2020.3011028

Mayron, L. M. (2015). Biometric authentication on mobile devices. IEEE Security &amp; Privacy, 13(3), 70–73. https://doi.org/10.1109/msp.2015.67

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys &amp; Tutorials*, *17*(3), 1268–1293. https://doi.org/10.1109/comst.2014.2386915

Phadke, S. (2013). The importance of a biometric authentication system. The SIJ Transactions on Computer Science Engineering &amp; Its Applications (CSEA), 01(04), 18–22. https://doi.org/10.9756/sijcsea/v1i4/0104550402

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614–634. https://doi.org/10.1147/sj.403.0614

Ratjeana Malatji, W., van Eck, R., & Zuva, T. (2020). Acceptance of biometric authentication security technology on mobile devices. *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*. https://doi.org/10.1109/imitec50163.2020.9334082

Roy, S., Matloob, S., Seetharam, A., Rameshbabu, A., O'Dell, W. C., & Davis, W. I. (2017). Biometrics data security techniques for portable mobile devices. INAE Letters, 2(3), 123–131. https://doi.org/10.1007/s41403-017-0026-8

Rui, Z., & Yan, Z. (2019). A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access*, *7*, 5994–6009. https://doi.org/10.1109/access.2018.2889996

Ryu, R., Yeom, S., Herbert, D., & Dermoudy, J. (2023). The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. *ICT Express*, *9*(6), 1183–1197. https://doi.org/10.1016/j.icte.2023.04.003

Saunders, M. N., & Thornhill, A. (2011). Researching sensitively without sensitizing: Using a card sort in a concurrent mixed methods design to research trust and Distrust. *International Journal of Multiple Research Approaches*, *5*(3), 334–350. https://doi.org/10.5172/mra.2011.5.3.334

Silasai, O., & Khowfa, W. (2020). The study on using biometric authentication on mobile device. NU. International Journal of Science, 17(1), 90-110.

Taha, M. A., Ahmed, H. M., & Husain, S. O. (2022). Iris Features Extraction and Recognition based on the Scale Invariant Feature Transform (SIFT). *Webology*, *19*(1), 171–184.

Tao, Q., & Veldhuis, R. N. J. (2006). Biometric authentication for a mobile personal device. 2006 3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops. https://doi.org/10.1109/mobiqw.2006.361741

Torres, J., de los Santos, S., Alepis, E., & Patsakis, C. (2020). User behavioral biometrics and machine learning towards improving user authentication in smartphones. Communications in Computer and Information Science, 250–271. https://doi.org/10.1007/978-3-030-49443-8_12

Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. Computer Networks, 170, 107118.

Wu, Q. (2014). Fingerprint Preprocessing and Recognition System Development and Design. *Advanced Materials Research*, *971-973*, 1897–1900. https://doi.org/10.4028/www.scientific.net/amr.971-973.1897