IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁒ Peer-reviewed & Refereed journal ⁒ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13486

# A STUDY ON DATA SECURITY ON MOBILE APPLICATION

**Dr. P. Kannan[1], Ms. T. Ilakkya[2], Mr. S. Abhishek[3]**

Professor, Department of Commerce (IT), Dr. N. G. P. Arts & Science College, Coimbatore.[1]

Student of B.Com IT., Dr. N. G. P. Arts & Science College, Coimbatore[2]

Student of B.Com IT., Dr. N. G. P. Arts & Science College, Coimbatore[3]

**Abstract:** The widespread adoption of mobile application has introduced significant data security risks, compromising sensitive use information. A mixed method approach was employed combining a literature review, survey of mobile application developer and users and vulnerability testing of selected mobile applications. The results reveal inadequate data security practices, including insecure data storage, insufficient encryption, and weak authentication mechanisms. This project provides recommendations for improving data security in mobile applications, emphasizing the need for robust security measures, user education, and awareness. The findings and recommendations contribute to the development of more secure mobile applications, benefiting developers, users, and organizations.

**Keywords:** Digital Security, Encryption

## I.INTRODUCTION

Data security refers to the practical and technologies design to protect digital information from unauthorised access.
In today’s digital world data is valuable asset that requires a comprehensive and strong set of measure designed to safeguard from various types of threats.
The rapid growth of mobile device and application has transformed the way we live, work and communication. However technology has introduced new security risk. Mobile app security is the practice of safeguarding high-value mobile applications and your digital identity from fraudulent attack in all its forms. This includes tampering, reverse engineering, malware, key loggers, and other forms of manipulation or interference.

## II.STATEMENT OF THE PROBLEM

Increasing threats to mobile data With the rise of mobile app usage, there is a growing risk of unauthorized access to sensitive personal data stored and transmitted through these applications.
Lack of robust encryption Many mobile apps do not implement strong encryption measures for storing or transmitting data, making it vulnerable to hacking, interception, and theft.
Insecure APIs Mobile applications often rely on APIs to communicate with servers. If these APIs are not secure, they can become entry points for attackers to compromise data integrity and user privacy.

## III.OBJECTIVES OF THE STUDY

1. Awareness of the data security in mobile application
- To educate users about the potential risk and threats associated with mobile application.

2. Types of tools
- To ensure data stored on mobile devices is encrypted and protected from unauthorized access using tools.
- To ensure only authorized users can access mobile application and data.

3. Identification of authorized in data security
- To identify malicious activity

## IV.RESEARCH METHODOLOGY

**RESEARCH AREA**
The research is conducted in Coimbatore.

DOI: 10.17148/IJIREEICE.2025.13486

**RESEARCH PERIOD**

The research is conducted over a period of 4 months from December 2024 to March 2025.

**NUMBER OF SAMPLES**

Sample size taken for the study is 114

**RESEARCH TOOLS**

For this study

1. Simple Percentage analysis

$$\text{PERCENTAGE} = \frac{\text{Number of respondents}}{\text{Total respondents}} \times 100$$

2. Chi-Square analysis

$$x^2 = \frac{(O - E)^2}{E}$$

## V.REVIEW OF LITERATURE

**1. Elisa Bertino,2012 -** Data security in mobile apps: Synthesis lectures on data security
**2. Cen et** Mobile app security risk assessment
**3. Malware and Trojans:** Mobile devices are susceptible to malware attacks, such as ransomware and spyware, which can steal sensitive information.
**4. End-to-End Encryption (E2EE):** According to Zhou et al. (2018), end-to-end encryption has become a standard practice for apps dealing with private messages, such as WhatsApp and Signal. This ensures that even if attackers intercept the data, they cannot read it without the decryption keys.
**5. Data Security: Yang & Xu (2019)** Discuss the security challenges of cloud integration, including the need for secure APIs, encryption, and access control.

## VI.DATA ANALYSIS, INTERPRETATION & INFERENCE

TABLE 1 DATA ANALYSIS IN GENDER

| S.NO | GENDER | PERCENTAGE |
|---|---|---|
| 1. | MALE | 38% |
| 2. | FEMALE | 62% |
| | TOTAL | 100% |

**INTERPRETATION**

The above table shows that female is the highest respondent of the gender at 62% &the lowest respondent is 38%.

TABLE 2 MOST COMMON TO AUTHENTICATE USERS

| S.NO | METHODS | PERCENTAGE |
|---|---|---|
| 1. | PIN | 14% |
| 2. | FACE RECOGNITION | 10% |
| 3. | PASSWORD | 34% |
| 4. | FINGER PRINT SCAN | 42% |
| | TOTAL | 100% |

**INTERPRETATION**

The above table shows that common methods to authenticate users on mobile app is the highest respondent on finger print scan with 42% and lowest respondent is 10%

DOI: 10.17148/IJIREEICE.2025.13486

TABLE 3 EXAMPLE FOR MOBILE SECURITY

| S.NO | EXAMPLES | PERCENTAGE |
|---|---|---|
| 1. | CROSS SITE SCRIPTING | 20.4% |
| 2. | SQL INJECTION | 20.4 |
| 3. | IMPROPERLY STRONG PASSWORDS | 28.6% |
| 4. | ALL THE ABOVE | 30.6% |
| | TOTAL | 100% |

**INTERPRECTION**
The above table shows that all the above with highest respondent 30.6% & SQL injection with lower respondent 20.4%

TABLE 4 TECHNIQUES UESD TO SECURE MOBILE APP

| S.NO | TECHNIQUES USED | PERCENTAGE |
|---|---|---|
| 1. | HTTP | 40.8% |
| 2. | SSL/TLS | 30.6% |
| 3. | FTP | 16.3% |
| 4. | TELNET | 12.3% |
| | TOTAL | 100% |

**INTERPRETATION**
The above table shows that HTTP is the highest respondent with 40.8% & the lowest respondent is 12.3%

TABLE 5 PURPOSE OF CODE OBFUSCATION

| S.NO | CODE OBFUSCATION | PERCENTAGE |
|---|---|---|
| 1. | PREVENT UNAUTHORIZED ACCESS TO DATA | 30.6% |
| 2. | MAKE THE APP HARDER | 28.6% |
| 3. | INCREASE THE SPEED | 28.6% |
| 4. | STORE DATA SECURELY | 12.2% |
| | TOTAL | 100% |

**INTERPRETATION**
The above table shows that prevent unauthorized access to data with highest respondent 30.6% & the lower respondent is 12.2%

## VII.CHI- SQUARE ANALYSIS

**HYPOTHESIS:**
**$H_0$** - There is no significant relationship between observed and expected frequencies of common authenticate users on mobile app.
**$H_1$** - There is a significant relationship between observed and expected frequencies of common authenticate users on mobile app.

Formula:

$$x^2 = \frac{(O-E)^2}{E}$$

O = Observed frequency
E = Expected frequency

**OBSERVED FREQUENCY TABLE**

| AUTHENTICATION METHOD | FREQUENCY |
|---|---|
| PIN | 16 |
| FACE RECOGNITION | 18 |
| PASSWORD | 35 |
| FINGER PRINT SCAN | 40 |
| TOTAL | 109 |

DOI: 10.17148/IJIREEICE.2025.13486

**EXPECTED FREQUENCY**

| AUTHENTICATION METHOD | PERCENTAGE | EXPECTED FREQUENCEY |
|---|---|---|
| PIN | 14.7% | 16 |
| FACE RECOGNITION | 16.5% | 18 |
| PASSWORD | 32.1% | 35 |
| FINGER PRINT | 36.7% | 40 |

**INFERENCE:**

- Since the **Chi-Square statistic (0.05)** is **greater** than the **critical value (7.815)**, we **reject the null hypothesis**.
- Based on the Chi-Square result, we conclude that authentication method preference is not equally distributed to respondents.
- Therefore it is concluded that there is a no strong evidence to suggest a significant in preferences.

## VIII.RECOMMENDATIONS

- Ensuring data security in mobile applications is crucial due to the sensitive nature of user information often stored or transmitted through these apps. Developers should begin by implementing strong encryption techniques such as AES for data at rest and TLS for data in transit, ensuring that personal and financial information is protected both on the device and across networks.
- Ensuring data security in mobile applications is crucial due to the sensitive nature of user information often stored or transmitted through these apps. Developers should begin by implementing strong encryption techniques such as AES for data at rest and TLS for data in transit, ensuring that personal and financial information is protected both on the device and across networks.

## IX.CONCLUSION

The study data security in mobile applications is a critical aspect that cannot be overlooked, given the increasing reliance on mobile devices for sensitive transactions and communication. The integration of robust security measures, such as encryption, secure authentication, and secure coding practices, helps protect user data from potential threats and breaches. Additionally, continuous monitoring and regular updates are essential to address new vulnerabilities and evolving attack methods. By prioritizing data security, developers can build trust with users, ensure compliance with privacy regulations, and ultimately enhance the overall user experience. In a rapidly changing digital landscape, maintaining strong data security is not just a best practice but a necessity to safeguard both users and organizations from potential risks.

## REFERENCES

1. "A Survey on Data Security in Mobile Applications" by S. S. Iyengar et al., published in the Journal of Network and Computer Applications, Vol. 124, 2019.
2. "Mobile Application Security: A Review" by A. K. Singh et al., published in the Journal of Information Security and Applications, Vol. 44, 2019.
3."Data Protection in Mobile Applications: A Survey" by R. K. Singh et al., published in the Journal of Mobile Information Systems, Vol. 2018.
4. "Security and Privacy in Mobile Applications: A Survey" by Y. Zhang et al., published in the Proceedings of the 2019 IEEE Conference on Communications and Network Security.
5. "A Study on Data Security in Mobile Applications" by S. K. Singh et al., published in the Proceedings of the 2018 International Conference on Information Technology.