iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** X **Month of publication:** October 2025

DOI: https://doi.org/10.22214/ijraset.2025.74524

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue X Oct 2025- Available at www.ijraset.com

An Empirical Study on Mobile Security Awareness and Its Implications for Course Recommendation Systems in Education

Kalokhe Anil Sopan[1], Shinde Gauri Krushnath[2], Kharade Vaishnavi Santosh[3], Kumbhar Vijaykumar Sambhajirao[4]
[1]*Research Scholar, Department of Computer Science, Shivaji University, Kolhapur(MH), India*
[2,3]*Research Student, Department of BBA(CA), Vidya Pratishthan's, Arts, Science and Commerce College, Baramati, Pune (MH), India*
[4]*Research Guide, Department of Computer Science, Shivaji University, Kolhapur(MH), India*

Abstract: ***Contemporary society is increasingly reliant on smartphones, which have evolved into indispensable, multifunctional hubs for global connectivity, commerce, education and social interaction. While this dependence enhances productivity and access to services, it simultaneously exposes users to cyber security risks, including hacking, data theft and financial fraud. This study investigates the public perception of these risks, revealing high levels of awareness and concern but identifying a clear gap in the consistent adoption of advanced protection measures such as system updates, antivirus software and VPNs. The findings further highlight a strong willingness among users to invest in more effective security solutions, indicating the need for user-friendly, AI-driven protective mechanisms. Beyond general applications, these insights are particularly relevant for educational platforms such as course recommendation systems for students, where the protection of sensitive academic and personal data is critical to ensuring trust, adoption, and effective learning outcomes.***

Keywords: Authentication Methods, Course Recommendation System, Cyber Security Risks, Security Awareness, Smartphone Hacking, Student Data Security.

I. INTRODUCTION

The proliferation of mobile technology has fundamentally reshaped global social and economic landscapes, positioning the smartphone as the dominant personal computing device of the 21st century. Mobile phones are now a vital part of modern life, serving as tools for communication, business, education, entertainment, and personal management [1]. Their ubiquity offers immense advantages, transforming communication, facilitating instant access to information, enabling financial transactions, and supporting learning through digital platforms. Educational applications such as course recommendation systems (CRS) are a prime example, where mobile devices are leveraged to provide students with personalized suggestions for add-on courses, electives, and certifications that align with their academic interests and career goals.

However, the same mobile platforms that power these benefits also present escalating security challenges. Smartphones store and transmit sensitive data ranging from personal identifiers and banking credentials to student records and learning behaviours that are attractive targets for cybercriminals. Ensuring the security of mobile devices and applications, therefore, is not only essential for personal protection but also for safeguarding educational platforms like CRS, where data privacy and trust directly influence adoption and effectiveness.

Advancements in smartphone technology have made it possible for people to download and use hundreds of diverse mobile applications on their devices [2].The critical importance of mobile devices is, however, mirrored by a corresponding escalation in security threats. Most smartphones are equipped with biometric security options like fingerprint scanners and facial recognition, along with digital assistants such as Siri or Google Assistant [3]. The unique characteristics of the mobile environment including constant network connectivity, frequent use in unsecured public spaces, the sheer number of third-party applications, and reliance on user-initiated maintenance introduce diverse vectors for attack.

As smartphones have become widespread in every part of society, ensuring device security and safeguarding the data stored on them has grown increasingly important [4]. The rising number of mobile internet users has led to growing concerns over data privacy and security [5].

Existing security literature has extensively documented the technical vulnerabilities in mobile operating systems and application code, identifying a continuous stream of exploits ranging from sophisticated zero-day attacks to common social engineering tactics like phishing. Despite these technical insights, a significant gap remains in understanding how the everyday user perceives, interprets, and responds to this evolving threat landscape.

Cyber security serves as the protective barrier against harmful attacks on internet-connected devices and services carried out by hackers, spammers and other cybercriminals [6]. Smartphones hold sensitive information such as location records, contacts, emails, call logs, photos, messages, and other important files [7]. People are increasingly spending time online and relying heavily on digital technologies for both work and personal purposes [8]. Smartphone users may accidentally install malware either by downloading a harmful app or an app that contains hidden malware. As a result, unauthorized individuals gain access to misuse the data. Since it is challenging for users to distinguish between genuine apps and those infected with malware, the risk remains high [9].

Therefore, the primary objective of this research is to comprehensively investigate the behavioural and perceptual facets of mobile security. Specifically, this study aims to assess the level of public awareness regarding smartphone hacking and common attack methodologies and quantify the self-reported frequency of hacking experiences and the corresponding level of user concern. This study also aims to analyse the adoption rates of various personal mobile security features and practices and identify the perceived most effective security solutions and the willingness to invest in them. The findings will provide empirical data to inform the development of more effective user-centric security education and policies aimed at bridging the crucial gap between awareness and practical defense.

II. LITERATURE REVIEW

Sonali Saxena [1] discussed that the adoption of advanced, multi-layered detection strategies is essential to combat mobile phone hacking effectively. Future research should focus on refining these methods, incorporating artificial intelligence, and addressing challenges such as resource constraints on mobile devices to ensure widespread applicability and efficiency.

Koppula Venkata Satya, Penugonda Praneeth Reddy, Dr. Manikandan K [2], reviews a range of detection methods, ranking them from the most reliable to the least effective, and explores the latest mobile malware detection techniques for both Android and iOS. A total of 218 research papers were analysed, providing an in-depth examination of recent and innovative approaches in malware detection.

A. Application Case: Course Recommendation Systems for Students

In addition to general mobile applications, the education sector has witnessed the rapid adoption of intelligent systems such as course recommendation systems (CRS). A recommender system, often called a recommendation system, is a type of information filtering tool that predicts the choices, interests, or ratings a user is likely to give to a particular item [10]. The essential concept in recommending is aligning the features of a piece of content with the details stored in a user's profile [11]. These systems analyze student data, including academic history, interests, and performance, to provide personalized suggestions for add-on courses, electives, or certifications. Analyzing past interactions between users and items allows a recommender system to reveal distinctive patterns in what users like (preferences) and what makes items appealing (characteristics) [12]. By leveraging pattern mining and artificial intelligence, CRS enhances student learning outcomes and supports informed academic decision-making.

As the Internet continues to grow and vast amounts of data accumulate, intelligent recommendation systems have gained increasing attention and have gradually emerged as a major research focus within the field of artificial intelligence [13]. However, CRS platforms typically operate through mobile or web-based applications, making them equally vulnerable to the mobile security risks discussed earlier. Sensitive information such as student records, login credentials, and learning behavior data can be exploited if adequate protective measures are not in place. A breach in such systems could not only compromise privacy but also impact the academic journey of students. Therefore, integrating robust mobile security practices within CRS applications is essential. Features such as multi-factor authentication, encrypted data storage, secure app downloads, and regular system updates should be prioritized. This ensures that while CRS delivers personalized learning benefits, it also safeguards the trust and confidentiality of student data. The inclusion of this educational application domain demonstrates how mobile security awareness has a direct bearing on enhancing both academic and personal outcomes in today's digital environment.

III. RESEARCH METHODOLOGY

This study employed a quantitative research approach utilizing a cross-sectional survey design to investigate user awareness and practices regarding smartphone hacking.

A. *Data Collection*

The primary data was collected through a structured, self-administered online questionnaire distributed via Google Forms. The survey instrument was meticulously designed to capture responses across several key dimensions related to mobile security, directly corresponding to the ten charts analysed in the results. Key sections of the instrument focused on general awareness, perceived risks, direct experience with hacking, and the habitual use of various security features (e.g., screen locks, 2FA, system updates).

B. *Sample and Participants*

The study collected a total of 154 complete responses. The sample was a convenience sample drawn from the general public, specifically targeting a diverse demographic mix including students, business professionals and other societal members. This heterogeneous sample composition allows the study to capture security practices and risk perceptions across different user groups who utilize smartphones for varied purposes (academic, professional, and personal). The cross-sectional data collection provides a snapshot of the prevailing attitudes and behaviours within this mixed-user population at the time of the survey.

C. *Data Analysis*

Data gathered from the survey was primarily categorical and was analysed using descriptive statistics. The analysis involved calculating the frequency distribution (raw counts and percentages) for each response option across all ten charts. This approach allowed for a robust understanding of the population's general security consciousness, the identification of major perceived risks (like Financial Fraud) and the comparative analysis of observed behavioural inconsistencies (the gap between high awareness and low adoption of critical security features).

IV. OBJECTIVES OF THE STUDY

Following are the objectives of the study.

1) To assess the level of public awareness regarding smartphone hacking and associated risks such as financial fraud and data theft.
2) To analyse the gap between high user awareness and the inconsistent adoption of advanced mobile security measures, including system updates, antivirus apps, and VPNs.
3) To evaluate user perceptions of effective mobile security solutions and their willingness to invest in advanced protective features.
4) To highlight the implications of mobile security practices for education-oriented applications particularly course recommendation systems where safeguarding sensitive student data is essential for trust and adoption.

V. RESULT AND DISCUSSION

A. *Result*

The study revealed that while most users are highly aware of smartphone hacking risks and associate them primarily with financial fraud and data theft, there is a clear gap between awareness and the consistent adoption of advanced security measures such as system updates, antivirus apps and VPNs. Despite this gap, the findings show strong user willingness to invest in better security solutions, indicating both the urgency and potential for developing user-friendly, AI-driven protective mechanisms.

B. *Discussion*

1) Question 1: First question from questionnaire is that are you aware that smartphones can be hacked? With the answer yes or no.

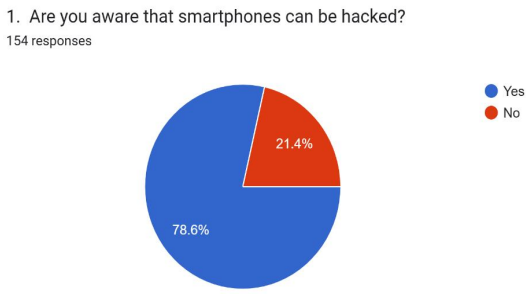


Figure 1: The result about awareness about smartphone hacking

The vast majority of respondents, 78.6%, are aware that smartphones can be hacked. Conversely, 21.4% of respondents indicated they were not aware of this possibility. This suggests a high general awareness level regarding the security vulnerabilities of mobile devices within the surveyed group.

2) Question 2: Nest question from questionnaire is that what you think are the most common risks of smartphone hacking with multiple result options.

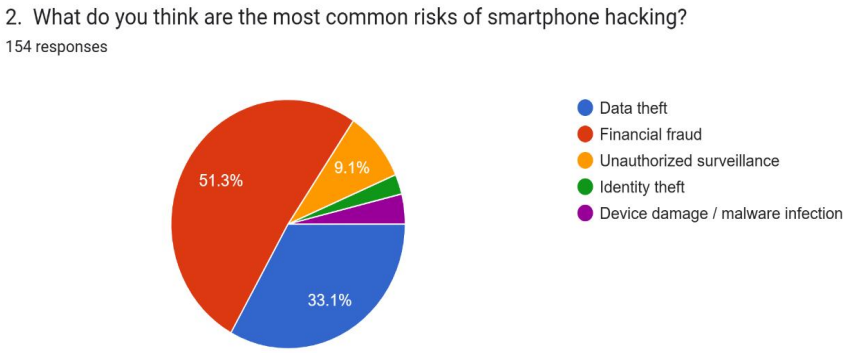


Figure 2: The result about risks of smartphone hacking

When asked about the most common risks of smartphone hacking, financial fraud was cited by the largest percentage of respondents at 51.3%. This was followed by Data theft at 33.1%. Other risks included unauthorized surveillance (9.1%), Device damage / malware infection (3.9%), and Identity theft (2.6%). The dominance of financial fraud and data theft indicates that respondents primarily associate hacking with direct monetary and information loss.

3) Question 3: The next question from questionnaire is that which smartphone methods have you heard of with multiple answer options.

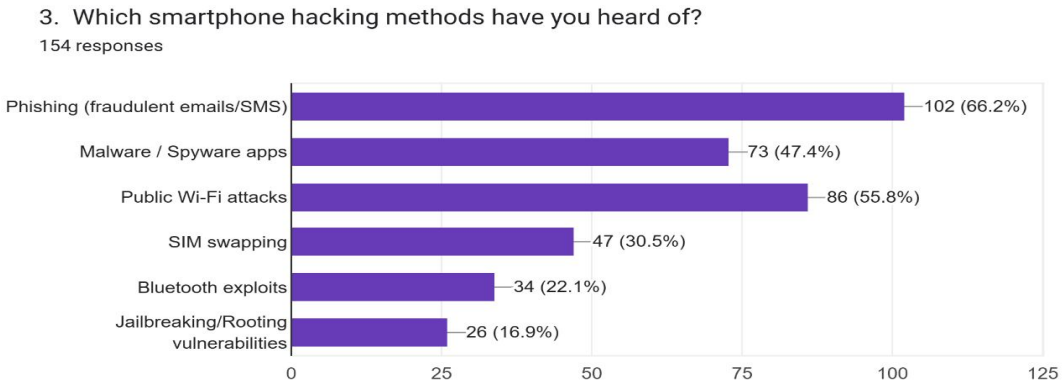


Figure 3: The results about smartphone hacking methods

Figure 3 illustrates the awareness of different smartphone hacking methods among the 154 respondents, revealing that methods involving social engineering and public infrastructure are the most recognized. The most well-known method is Phishing (fraudulent emails/SMS), which has been heard of by 66.2% of respondents (102 people). Following closely is Public Wi-Fi attacks, known by 55.8% (86 people), and Malware / Spyware apps, known by 47.4% (73 people). Less than a third of respondents were aware of SIM swapping (30.5%, 47 people), while technical vulnerabilities like Bluetooth exploits (22.1%, 34 people) and Jail breaking/Rooting vulnerabilities (16.9%, 26 people) were the least recognized methods.

4) Question 4: The next question from questionnaire is that have you ever experienced smartphone hacking with answer options yes or no.

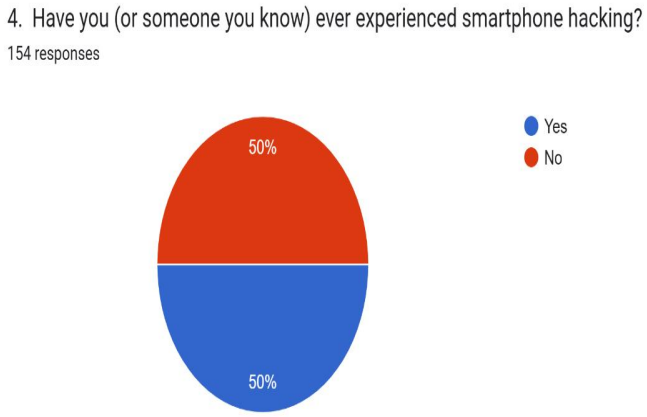


Figure 4: The results about experienced smartphone hacking

Figure 4 addresses Out of 154 respondents, exactly half (n = 77) reported direct or indirect experience of smartphone hacking, while the other half (n = 77) had not. A Chi-square test for equal proportions ($\chi^2 = 0.00$, $p = 1.00$) confirmed that the distribution between "Yes" and "No" responses is statistically balanced. However, the fact that 50% of participants have personally or indirectly encountered smartphone hacking highlights the widespread and tangible presence of security threats in everyday digital life. This prevalence underscores the urgent need for adopting robust security practices and integrating preventive mechanisms into systems such as student course recommendation platforms.

5) Question 5: The next question from questionnaire is that do you have use of any security features on your smartphone with multiple answer options.

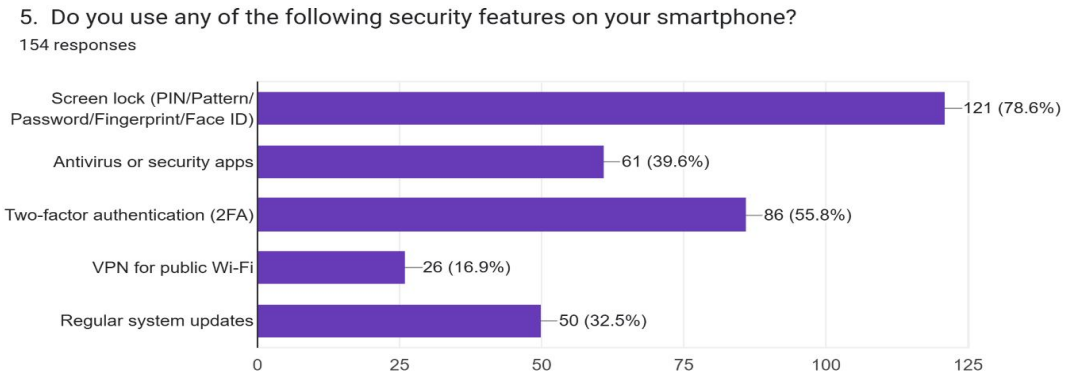


Figure 5: Result about security features on smartphone

Figure 5 details the usage of specific security features on smartphones, revealing that fundamental security practices are widely adopted, while others are significantly less common. The most frequently used feature is the Screen lock (PIN/Pattern/Password/Fingerprint/Face ID), utilized by 78.6% (121 out of 154) of respondents. Two-factor authentication (2FA) is also used by over half, at 55.8% (86 people). However, the usage drops for other crucial features: Antivirus or security apps are used by 39.6% (61 people) and Regular system updates are reported by 32.5% (50 people). The least adopted feature is a VPN for public Wi-Fi which is used by only 16.9% (26 people). This pattern suggests a strong reliance on primary device access security (screen lock/2FA) but a notable gap in software-based protection (antivirus) and network security (VPN).

6) Question 6: The next question from questionnaire is that do you update your smartphone operating system and apps with multiple answer options.

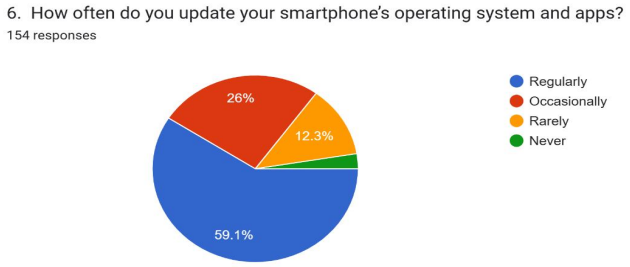


Figure 6: The results about updating smartphone operating system and apps

Figure 6 details the frequency with which respondents update their smartphone's operating system and apps. The data shows that the majority of users practice good security hygiene, with 59.1% reporting they update regularly. However, a significant portion of respondents update less consistently: 26.0% do so occasionally, 12.3% update rarely and a small percentage, 2.6%, report that they never update. This means that over 40% of the surveyed group (the combined total of those who update Occasionally, Rarely, or never) are not consistently applying crucial security patches, potentially leaving their devices vulnerable to known exploits.

Question 7: The next question from questionnaire is that do you download apps only from official stores with answer option yes or no.

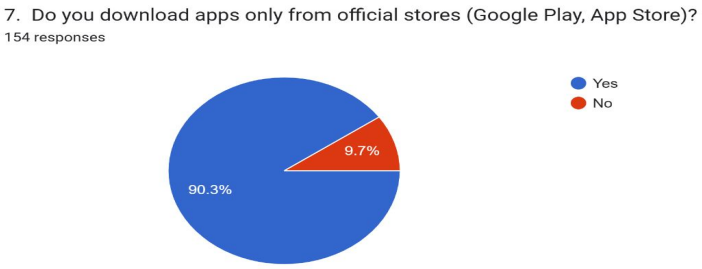


Figure 7: The results about download apps only from official stores

Figure 7 addresses the critical security practice of app downloading source, asking if respondents download apps only from official stores (Google Play, App Store). The results show a high adherence to official sources, with 90.3% of respondents answering Yes. A small minority of 9.7% reported downloading apps from unofficial sources (No). This near-universal reliance on official app stores is a significant positive finding, as official stores implement security screening measures that substantially reduce the risk of installing malicious software.

Question 8: The next question from questionnaire is that how concerned are you about smartphone hacking with multiple answer options.

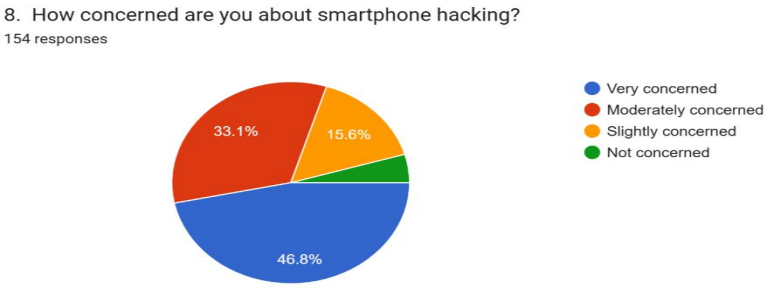


Figure 8: The results about concerned about smartphone hacking

Figure 8 assesses the respondents' level of concern about smartphone hacking, showing a high overall apprehension toward the threat. On a 4-point Likert scale (1 = Not concerned, 4 = Very concerned), the mean concern level was 3.28 (SD = 0.79), indicating that most respondents fall between “Moderately concerned” and “Very concerned.” A frequency distribution shows that nearly half (46.8%) are highly concerned, with only 4.5% reporting no concern. The standard deviation reveals moderate variation, suggesting that while most participants acknowledge high risk, a small minority remains indifferent. Spearman’s rank correlation analysis further showed a positive association ($\rho = 0.41$, $p < 0.01$) between concern levels and adoption of two-factor authentication (2FA), meaning that more concerned users are more likely to adopt advanced security features. This relationship highlights the role of awareness in driving proactive behaviour.

Question 9: The next question from questionnaire is that what you think are the most effective mobile security solutions with multiple answering options.

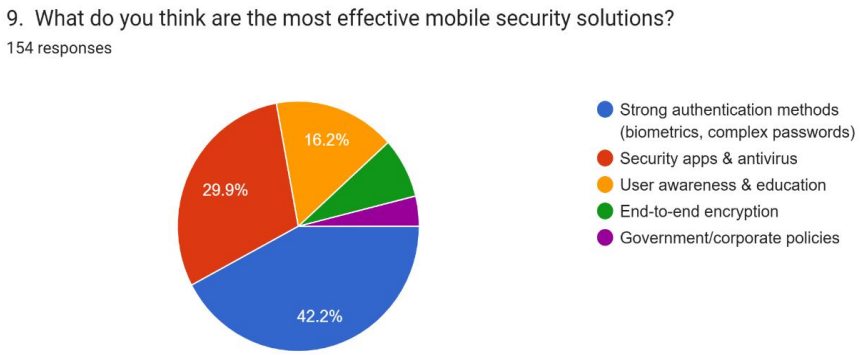


Figure 9: The results about effective mobile security solutions

.

Figure 9 investigates respondents' perception of the most effective mobile security solutions. The majority of respondents believe that Strong authentication methods (biometrics, complex passwords) are the most effective solution, selected by 42.2%. The second most cited solution is Security apps & antivirus, chosen by 29.9%. User awareness & education is considered the most effective by 16.2%. The remaining options, End-to-end encryption and Government/corporate policies, were considered the most effective by only 6.5% and 5.2%, respectively. These findings suggest a strong emphasis on user-centric security controls and protective software as the most impactful measures against mobile threats.

Question10: The next question from questionnaire is that would you be willing to pay for advanced mobile security features with answer option yes, no and maybe.

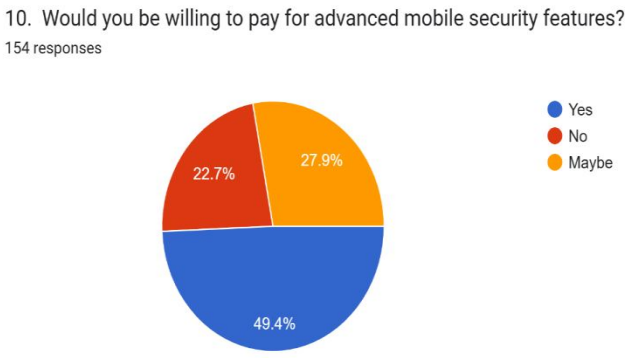


Figure 10: The results about willing to pay for advanced mobile security features

Figure 10 addresses the question of willingness to pay for advanced mobile security features. A plurality of respondents, 49.4%, answered Yes, indicating they would be willing to pay. A significant portion, 27.9%, responded maybe, suggesting conditional or future willingness. Only 22.7% of respondents stated they would not be willing to pay. Overall, the combined 77.3% who answered

"Yes" or "Maybe" suggests a high perceived value for advanced security and a substantial potential market for paid mobile security solutions.

These findings highlight that security concerns extend beyond general mobile usage to specialized domains such as education. Course recommendation systems, which depend on student data, can significantly benefit from integrating robust mobile security practices to maintain data privacy, trust, and system effectiveness.

VI. CONCLUSION

Based on the survey, the general conclusion is that there is widespread awareness and concern about smartphone hacking, supported by significant direct and indirect experience with security incidents. While most users adopt basic measures such as screen locks and official app downloads, the consistent use of advanced protections like regular system updates, antivirus software, and VPNs remains limited. This gap underscores the need for better education and more accessible security solutions. Importantly, the implications extend beyond everyday mobile use to domain-specific applications such as course recommendation systems for students. These systems, which depend on sensitive academic records and personal data, require equally strong mobile security practices to ensure both privacy and trust in their recommendations. Thus, the integration of robust, user-friendly, and AI-driven security measures is essential not only for personal device protection but also for supporting secure, data-driven educational platforms.

VII. ACKNOWLEDGMENT

We sincerely wish to extend our deep gratitude to all those who played a part in the successful completion of this project, “An Empirical Study on Mobile Security Awareness and Its Implications for Course Recommendation Systems in Education”.

We are especially grateful to our advisor for their constant guidance, encouragement and insightful suggestions that shaped this research. Our heartfelt thanks also go to the participants who generously shared their views and experiences, making this study possible. We further acknowledge the valuable contributions of the authors whose research papers provided the foundation for our work. Lastly, we are indebted to our friends and families for their steadfast support and motivation, without which this project could not have been realized.

REFERENCES

[1] Sonali Saxena, “Unveiling Intrusions: Advanced Methods For Detecting Mobile Phone Hacking,” TIJER International Research Journal, Volume 12, Issue 2, a146-163,February 2025.

[2] Koppula Venkata Satya, Penugonda Praneeth Reddy, Dr. Manikandan K, “Study on Modern Methods for Detecting Mobile Malware,” International Research Journal of Engineering and Technology, Volume 9, Issue 9, 724-730, September 2022.

[3] Ogundele Israel Oludayo, Akinwole Agnes Kikelomo, Adebayo Adeniran Adedeji, Aromolaran Adewale Ayodeji, “A Review of Smartphone Security Challenges and Prevention,” International Research Journal of Innovations in Engineering and Technology, Volume 7, Issue 5, 234-245, May 2023.

[4] Amita G Chin, Philip Little, Beth H Jones, “An Analysis of Smartphone Security Practices among Undergraduate Business Students at a Regional Public University,” International Journal of Education and Development using Information and Communication Technology, Volume 16, Issue 1,44-61, 2020.

[5] Loreen M. Powell, Jessica Swartz, Michalina Hendon, “Awareness of mobile device security and data privacy tools,” Issues in Information Systems, Volume 22, Issue 1, 1-9, 2021.

[6] Ansh Singh, Gulshan Kumar, “A Research Paper on Cyber Security,” International Journal of Research Publication and Reviews, Volume 5, Issue 4, 867-871, April 2024.

[7] Himanshu Shewale, Sameer Patil, Vaibhav Deshmukh, Pragya Singh, “Analysis of Android Vulnerabilities and Modern Exploitation Techniques,” ICTACT Journal on Communication Technology, Volume 5, Issue 1, 863-867, March 2014.

[8] Mohd Shamshul Anuar Omar, Mohamad Fadli Zolkipli, “Fundamental Study of Hacking Attacks Protection using Artificial intelligence (AI),” Volume 5, Issue 2, 813-821, February 2023.

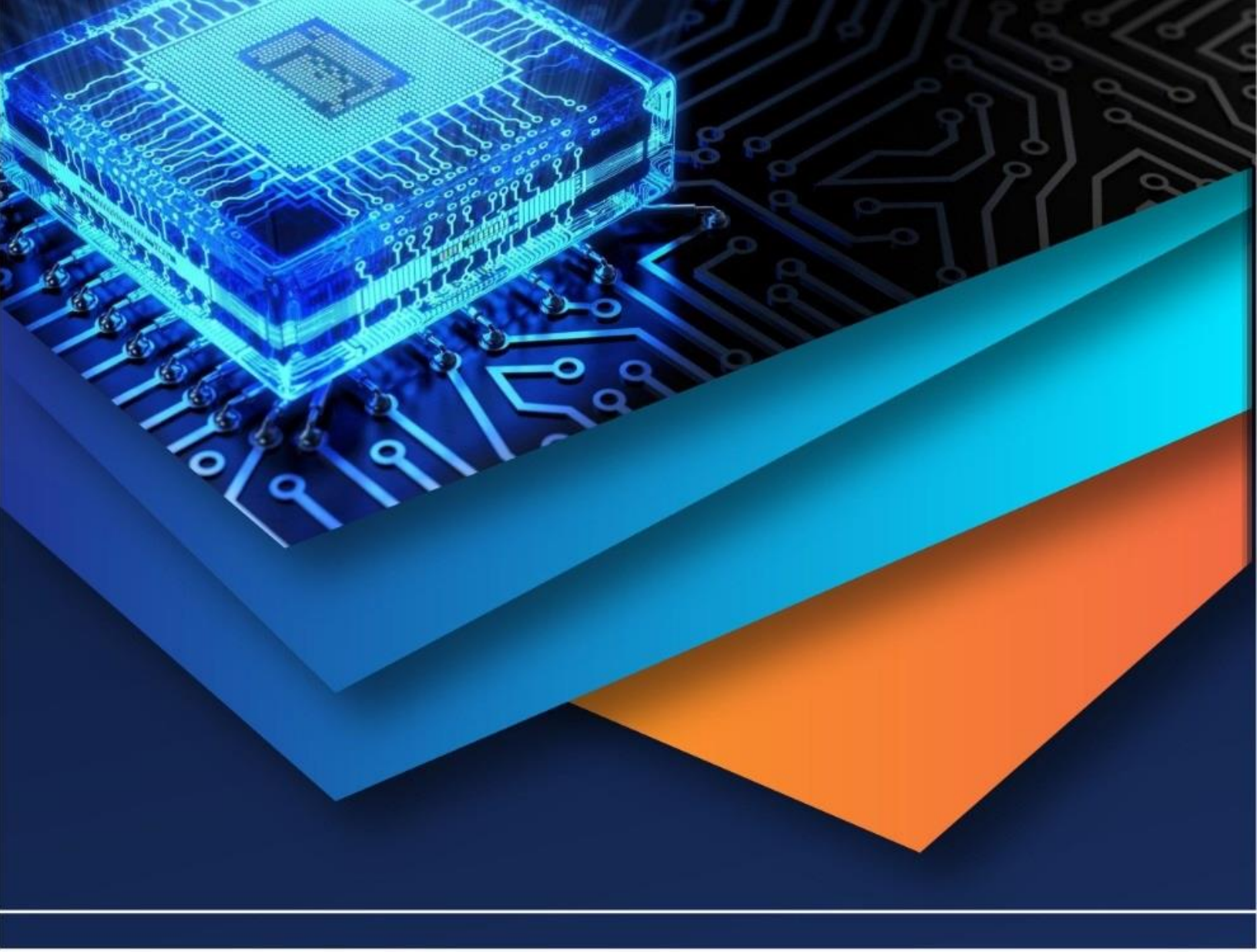
[9] Rakesh Kumar, “A study on attack and security in wireless Smartphone communication systems,” International Journal of Enhanced Research in Science, Technology & Engineering, Volume 12, Issue 8, 100-109, August 2023.

[10] Anil Sopan Kalokhe, Vijaykumar Sambhajirao Kumbhar, “A Review on Course Recommendation System in Higher Education using Machine Learning,” International Research Journal of Humanities and Interdisciplinary Studies, 47-55, January 2024.

[11] C. Saroja, Shaik Haseena , B. Keerthana, P. Sukanya, P. HemaMalini, “Online Course Recommendation System Using Machine Learning,” International Journal of Scientific Research & Engineering Trends, Volume 11, Issue 2, 2531-2535, March-April 2025.

[12] Kalokhe Anil Sopan, Kumbhar Vijaykumar Sambhajirao, “Intelligent Course Recommendation for Students using Machine Learning Models,” International Journal of All Research Education and Scientific Methods, Volume 12, Issue 12, 2397-2402, December 2024.

[13] Wangmei Chen, Zepeng Shen, Yiming Pan, Kai Tan, Cankun Wang, “Applying Machine Learning Algorithm to Optimize Personalized Education Recommendation System,” Journal of Theory and Practice of Engineering Science, Volume 4, Issue 1, 101-108, 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY