JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Balancing Security and Privacy in the Digital Era: A Study on Public Awareness and Technological Ethics

[1]Kalokhe Anil Sopan, [2]Phadtare Siddhi Dnyaneshwar, [3]Kale Samiksha Santaram, [4]Gunjawate Poonam Umesh,

[5]Kumbhar Vijaykumar Shambhajirao

[1]Research Scholar, [2, 3]Research Student, [4]Assistant Professor, [5]Research Guide
[1]Department of Computer Science, Shivaji University, Kolhapur (MH), India
[2,3]Department of BBA(CA), Vidya Pratishthan's, Arts, Science and Commerce College, Baramati, Pune (MH), India
[4]Assistant Professor, Department of BBA(CA), Vidya Pratishthan's Arts Science and Commerce College, Baramati(MH), India.
[5]Department of Computer Science, Shivaji University, Kolhapur (MH), India

Abstract: The study explores the intricate relationship between security and privacy in the digital era, emphasizing their interdependent role in safeguarding personal and organizational information. With the rapid rise of mobile technologies, online platforms, and data-driven systems, ensuring secure and private digital environments has become a critical necessity. The research investigates public perceptions of privacy and security, identifying key principles and technological concerns shaping the current discourse. It highlights the importance of maintaining a balanced approach that protects individual rights while ensuring societal safety through effective digital governance and ethical technology use. Widespread use of mobile technology has transformed the way individuals.

***Keywords*- Cyber Awareness, Data Protection, Digital Technology, Privacy, Security.**

I. INTRODUCTION

Security and privacy have become central concerns in the digital era, especially with the rapid adoption of technology-driven platforms such as mobile banking, e-learning systems, and online services. People are spending more time on the internet and becoming increasingly dependent on digital technologies for their professional and personal activities[1]. As users increasingly rely on digital tools for everyday tasks, safeguarding personal and financial information has emerged as a fundamental requirement. Security refers to the protection of data and systems from unauthorized access, alteration, or destruction, while privacy focuses on ensuring that individuals' personal information is collected, used, and shared responsibly. Together, these two aspects form the foundation of trust between users and digital service providers. Cyber security is the practice of preventing unauthorized access, misuse, or harm to computer systems, networks, data, and digital information [2].

Maintaining strong security and privacy measures involves implementing robust authentication methods, encryption techniques, and user awareness initiatives. As cyber threats evolve, traditional password-based systems are often insufficient to prevent unauthorized access. Online security has become a crucial element in shaping new technologies, digital services, and government regulations [3]. Biometric authentication, multi-factor verification, and advanced encryption protocols have become vital in strengthening digital defenses. A robust authentication mechanism is vital to protect user information and online accounts from cyber-attacks [4]. Furthermore, organizations must regularly update their systems and policies to address vulnerabilities and comply with privacy regulations.

The field of privacy-preserving technologies is continuously advancing, bringing innovations that transform the standards of security and data protection [5]. Data privacy, recognized as a basic human right, depends on protecting individuals' personal information to shield them from unauthorized access, exploitation, and unfair treatment [6]. Cybercrime refers to any criminal activity that involves the use of computers or networks [7]. Gathering and analyzing large volumes of personal information create major privacy issues, especially when people have limited control over how their data is utilized or distributed [8]. Tackling data security and privacy issues in the digital era demands a comprehensive and multi-dimensional strategy [9].

Equally important is the human aspect of security and privacy. Users play a critical role in maintaining digital safety through responsible online behavior, such as avoiding suspicious links, managing permissions, and protecting login credentials. Awareness and education initiatives are therefore essential to promote a culture of cyber security. In essence, ensuring security and privacy is not merely a technical necessity but a shared responsibility among individuals, organizations, and policymakers to create a safer and more trustworthy digital environment. Data privacy, also known as information privacy, refers to an individual's right to control the collection, use, and sharing of their personal information [10].

Privacy refers to any personal data related to an individual's behavior, finances, biometrics, health, or biographical details that are obtained through business analytics [11]. The widespread use of social media on the internet has led to an extraordinary surge in the amount of data accessible[12]. The growing dependence on technology highlights the need for continuous evaluation of how security and privacy are implemented and perceived in different digital domains. As users engage with online systems for education, banking, communication, and entertainment, their awareness and understanding of digital safety become crucial factors in shaping a secure virtual environment. Hence, exploring how individuals interpret and balance these two interlinked concepts provides valuable insights for improving digital governance, developing effective policies, and fostering responsible digital citizenship.

II. Literature Review

Kalokhe Anil Sopan, Shinde Gauri Krushnath, Kharade Vaishnavi Santosh, Kumbhar Vijaykumar Sambhajirao[1], stated that there is a broad awareness and concern regarding smartphone hacking, often reinforced by personal or observed experiences with security breaches. While many users implement basic safeguards like screen locks and downloading apps from official sources, the regular use of more advanced protections such as system updates, antivirus programs, and VPNs remains relatively uncommon.

Atul Arun Patil [2], discussed that Cybersecurity challenges and threats are constantly evolving, posing significant risks to individuals, businesses, and organizations. A complex and critical cyber landscape has emerged due to rapid technological advancements and the growing interconnection of systems and networks. As more systems are developed, the potential points of attack increase, giving cybercriminals additional opportunities to exploit vulnerabilities.

III. Research Methodology

The study employed a quantitative research design using a structured cross-sectional survey to gather insights from respondents regarding their understanding of security and privacy. A well defined questionnaire was developed to capture perceptions, attitudes, and awareness related to digital protection mechanisms and the ethical implications of data handling. The responses were systematically analyzed to interpret emerging trends and opinions, enabling a comprehensive understanding of the dynamic relationship between privacy and security in the modern digital context. This methodology ensured objectivity, reliability, and clarity in drawing meaningful conclusions from participant responses.study adopted a quantitative research approach using a cross-sectional survey design to performance trends.

IV. Objectives of the Study

1. To examine the interrelationship between security and privacy in the context of modern digital technologies and understand how they collectively influence user trust and data protection.
2. To analyze public awareness and perceptions regarding the importance of maintaining both security and privacy across online platforms and digital services.
3. To identify the key principles and technologies such as encryption, biometric systems, and artificial intelligence that shape current security and privacy practices.
4. To evaluate the challenges and ethical implications associated with balancing data security and individual privacy in technology-driven environments.
5. To recommend strategies and policy measures that promote a balanced, transparent, and responsible digital ecosystem ensuring both user safety and privacy preservation.

V. Result and Discussion

Result:

The study found a strong public understanding that security and privacy are interconnected and essential for digital trust. Respondents primarily associate privacy with protecting individual's personal information and security with ensuring the safety of citizens and national interests. The results clearly show a consensus that the absence of security leads to an unsafe and chaotic society, while the potential for an authoritarian state is the main concern when privacy is absent. Facial recognition and AI are overwhelmingly seen as the biggest technological threats to both concepts. The findings emphasize the need for continuous public awareness and education on digital protection mechanisms like encryption.

Discussion:

Question 1: The first question from questionnaire is that why are security and privacy described as two sides of the same coin with multiple options.

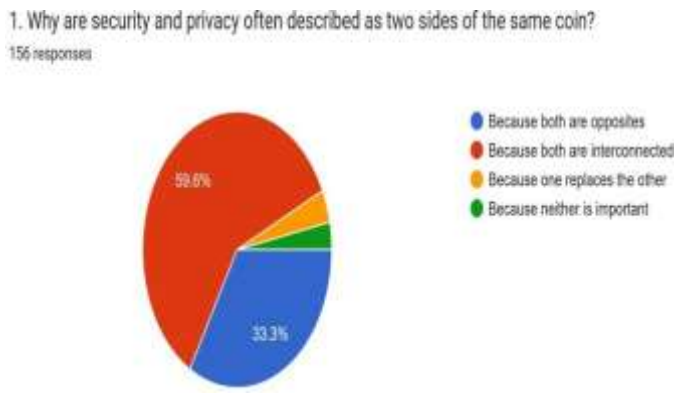

Figure 1: The result about security and privacy often described as two sides of the coin

The chart shows that most respondents (59.6%) believe security and privacy are interconnected, emphasizing their complementary role in protecting information. About 33.3% view them as opposites, reflecting the perceived balance between the two concepts. Only a small percentage thinks one replaces the other or that neither is important. Overall, the findings highlight a strong understanding of the close relationship between security and privacy.

Question 2: The nest question is that what privacy mainly protects with multiple options.

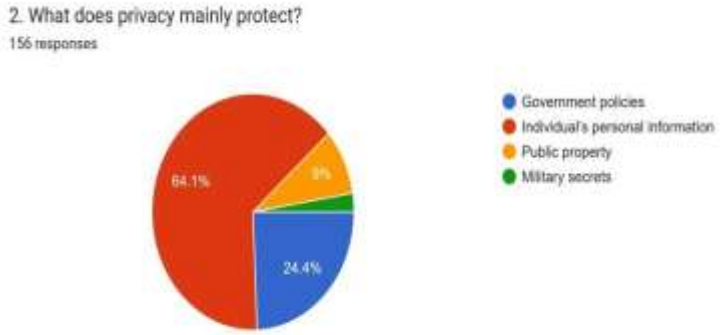

Figure 2: The result about privacy mainly protect

The chart indicates that a majority of respondents (64.1%) believe privacy primarily protects an individual's personal information, emphasizing the importance of safeguarding personal data in the digital era. About 24.4% associate privacy with protecting government policies, while 9% link it to public property. Only a small fraction considers military secrets as the main concern. Overall, the responses highlight a strong awareness of privacy as a personal right rather than an institutional or state concern.

Question 3: The next question is that what does security ensure with multiple option given.

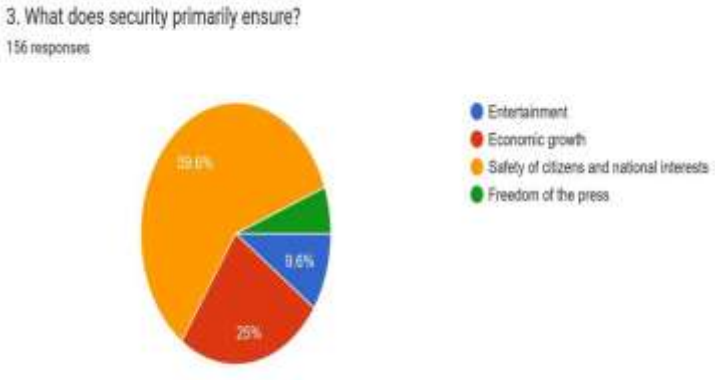

Figure 3: The results about does security primarily ensure

The chart reveals that a majority of respondents (59.6%) believe security primarily ensures the safety of citizens and national interests, highlighting its vital role in maintaining stability and protection. Around 25% associate security with economic growth, indicating awareness of its broader societal impact. A smaller portion (9.6%) connects it with entertainment, while a minimal number link it to freedom of the press. Overall, the responses emphasize security's central function in safeguarding people and national welfare.

Question 4: The next question is that what happens if a society has privacy but no security with multiple option.

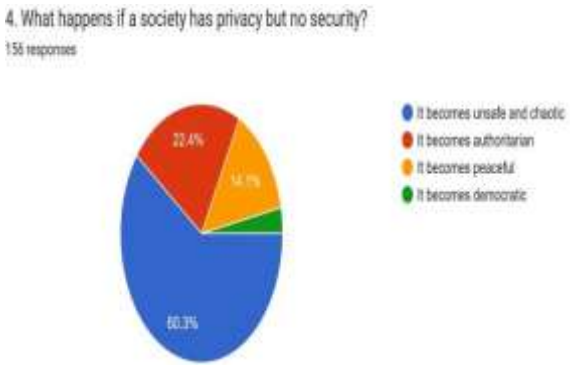

Figure 4: The results about happens if a society has privacy but no security

Based on the survey of 156 responses, the overwhelming majority (60.3%) believe that a society with privacy but no security would become unsafe and chaotic. A notable portion (22.4%) also expressed the concern that it could lead to an authoritarian state. In contrast, a much smaller group holds a positive outlook, with 14.1% thinking it would become peaceful. The prevailing sentiment clearly indicates that respondents view security as essential for a stable and safe society, even when privacy is guaranteed.

Question 5: The next question is that what happens if a society has security but no privacy with multiple options.

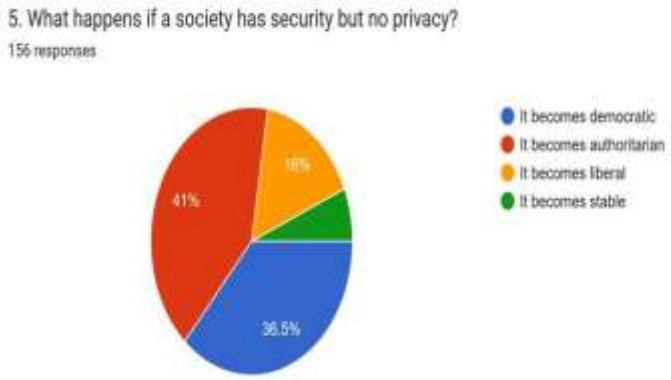

Figure 5: Result about happens if a society has security but no privacy

Based on the 156 responses, the public is divided on the outcome of a society with security but no privacy. The largest percentage, 41%, believes such a society would become authoritarian. However, a close second, at 36.5%, holds the opposing view that it would become democratic. A smaller, yet significant, portion of 16% suggests it would become liberal. The near-even split between 'authoritarian' and 'democratic' indicates a strong disagreement on whether total security at the expense of privacy promotes control or stability.

Question 6: The next question is that which principle guides the balance between privacy and security with multiple option given.

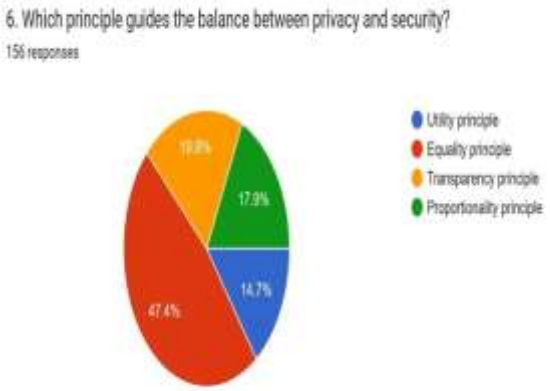

Figure 6: The results about principle guides the balance between privacy and security

Based on the survey of 156 responses, the public overwhelmingly believes the Equality principle (47.4%) is the most important for guiding the balance between privacy and security. The second most chosen principle is Transparency principle (19.9%), followed by the Proportionality principle (17.9%). The Utility principle received the least support at 14.7%. The results suggest

that fairness and equal application of rules are considered the most crucial factor in navigating the trade-off between privacy and security.

Question 7: The next question is that which technology raises the biggest concerns for both privacy and security today with multiple options given.

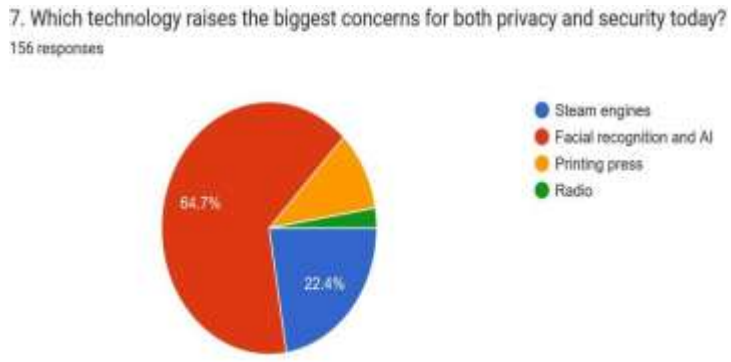

Figure 7: The results about technology raises the biggest concerns for privacy and security

Based on the survey of 156 responses, the public overwhelmingly identifies Facial recognition and AI as the technology raising the biggest concerns for both privacy and security today, with 64.7% of the vote. This highlights a clear modern anxiety about surveillance and automated decision-making. Notably, Steam engines received a surprisingly high 22.4% of the responses. The historical technologies, the Printing press and Radio, were largely dismissed, confirming that contemporary data technologies are the main focus of current privacy and security fears.

Question 8: The next question is that which international law focuses heavily on data privacy with multiple options given.

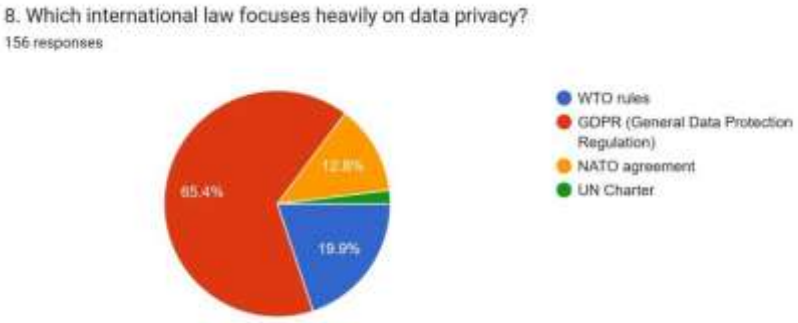

Figure 8: The results about international law focuses heavily on data privacy

Based on the survey of 156 responses, there's a strong consensus that the GDPR (General Data Protection Regulation) is the international law most focused on data privacy, with an overwhelming 65.4% of the responses. WTO rules were the second most selected option at 19.9%, though they primarily govern trade, not privacy directly. The NATO agreement and the UN Charter were considered significantly less relevant. This data clearly reflects the GDPR's status as the globally recognized benchmark for data protection.

Question 9: The next question is that which indian system sparked debates about privacy and security with multiple options.

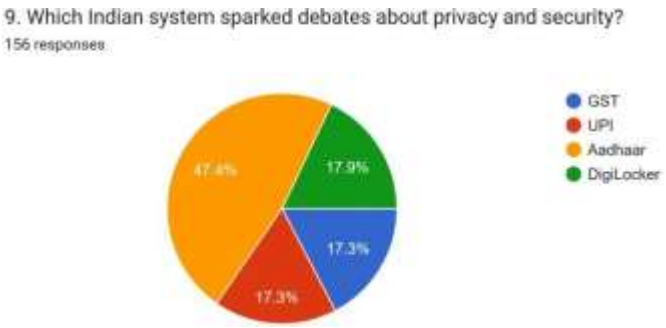

Figure 9: The results about indian system sparked debates about privacy and security

Based on the 156 responses, the Aadhaar system is overwhelmingly identified as the Indian system that has most sparked debates about privacy and security, capturing 47.4% of the responses. This result confirms its central role in India's data governance discussions. The remaining options, GST, UPI, and DigiLocker, received significantly less but comparable attention, with 17.3%,

17.3%, and 17.9% respectively. The data clearly shows that the national identity project, Aadhaar, is the primary source of public concern regarding the privacy-security trade-off in India.

Question10: The last question is that which of the following helps in protecting digital privacy with option spyware, encryption, key loggers and CCTV cameras.

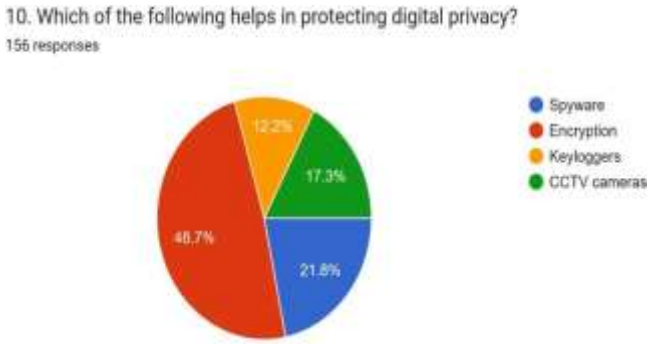

Figure 10: The results about techniques help in protecting digital privacy

Based on the survey of 156 responses, nearly half the participants, 48.7%, correctly identified Encryption as the technology that helps in protecting digital privacy. However, a significant number of respondents incorrectly chose harmful or surveillance-focused options. Specifically, Spyware was selected by 21.8% and CCTV cameras by 17.3%. Keyloggers were chosen by 12.2%. This suggests that while there is an awareness of encryption's role, a large portion of the public may misunderstand common digital security concepts.

VI. Conclusion

The research concludes that both security and privacy are essential, interdependent pillars of digital trust. While security safeguards systems and information from unauthorized access, privacy ensures that individual data is handled responsibly and ethically. The findings underline the need for continuous awareness, education, and policy development to address emerging technological challenges such as artificial intelligence and biometric surveillance. Ultimately, fostering a balance between security and privacy is vital for sustaining user confidence, protecting democratic values, and promoting a safer digital ecosystem.

Acknowledgment

The authors express their sincere gratitude to all individuals who contributed to the successful completion of this research. We extend our appreciation to the participants for their valuable responses and cooperation, which greatly enhanced the quality of the study. Special thanks are also due to peers and mentors for their constructive suggestions, encouragement, and guidance throughout the research process. Finally, we are thankful to our families and friends for their constant support, motivation, and understanding during the preparation of this work.

References

[1] Kalokhe Anil Sopan, Shinde Gauri Krushnath, Kharade Vaishnavi Santosh, Kumbhar Vijaykumar Sambhajirao, "An Empirical Study on Mobile Security Awareness and Its Implications for Course Recommendation", *International Journal for Research in Applied Science & Engineering Technology*, Volume 13 , Issue 10, pp. 507-514, October 2025.

[2] : Atul Arun Patil, "Research Paper on Cyber Security Challenges and Threats," *International Journal of Advanced Research in Science, Communication and Technology*, Volume 4 , Issue 1, pp. 561-566, January 2024.

[3] : Wasyihun Sema Admass,Yirga Yayeh Munay ,Abebe Abeshu Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Application*, October 2023, https://doi.org/10.1016/j.csa.2023.100031.

[4] : Kalokhe Anil Sopan, Tamhane Pragati Gorakh, Babar Lavannya Ganesh, Pawar Mahesh Dattatray, "EA Study on user Awareness and Preferences for Authentication Techniques in Mobile Banking Applications," *International Journal of Innovative Research in Computer and Communication Engineering*, Volume 13 , Issue 10, pp. 15984-15991, October 2025.

[5] : Preston Mwiinga, "Privacy-Preserving Technologies: Balancing Security and User Privacy in the Digital Age," *International Journal of Scientific and Research Publications*, December 2023, DOI: 10.5281/zenodo.10406538.

[6] : Harsha Patil, Vikas Mahandule, Juber Fakir, Omprasad Ajgaonkar, "Balancing Data Privacy and Ethics in the Age of Big Data:Challenges and Solutions," Journal of Innovations in Business and Industry, Volume 3 , Issue 1, pp. 1-6, May 2024.

[7] : Kalokhe Anil Sopan, Pawar Mahesh Dattatray, Shinde Suraj Mohan, "Study on Frauds in Social Media: A Review," *Aayushi International Interdisciplinary Research Journal*, Special Issue 68, pp.528-531, February 2020.

[8] : Msbah J. Mosa, Alaa M. Barhoom, Mohammed I. Alhabbash, Fadi ES Harara, Bassem S. Abu-Nasser, and Samy S. Abu-Naser, " AI and Ethics in Surveillance: Balancing Security and Privacy in a Digital World," *International Journal of Academic Engineering Research*, Volume 8 , Issue 10, pp. 8-15, October 2024.

[9] : Aris Sarjito, " Data Security and Privacy in the Digital Era: Challenges for Modern Government ," *Jurnal Ilmiah Administrasi Negara*, 8 (3), pp. 01 – 13,August 2024.

[10] : Shivam Singh, "Exploring the Ethics of Data Privacy in the Digital Age," *Darpan International Research Analysis*," Volume 12 , Issue 3, pp. 216-227, July-September 2024.

[11] : Yasser A. AlQahtani, Adel A. Marghalani, "Digital Ethics and Privacy: A study about digital ethics issues, implications, and how to solve them," *International Journal of Computer Science and Information Technology Research*, Volume 7 , Issue 2, pp. 1-6, April- June 2019.
[12] : Kalokhe Anil Sopan, Pawar Mahesh Dattatray, "A Study on Data Mining Techniques in Social Media Data: A Review," *Aayushi International Interdisciplinary Research Journal*, Special Issue 49, pp. 480-485.