A Study on the Emerging Technologies and Data Privacy Challenges in India

AUTHOR

AKATHIYAN R

BBA LL.B (Hons)

SAVEETHA SCHOOL OF LAW

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES (SIMATS)

CHENNAI 600 077.

EMAIL ID : akathyan2002@gmail.com

CO AUTHOR

SANJANA. G

BBA LL.B (Hons)

SAVEETHA SCHOOL OF LAW

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES (SIMATS)

Chennai 600 077.

Email ID: sanjanasaigiri@gmail.com

ABSTRACT:

The world of technology in India has really blown up lately with new things like Artificial Intelligence (AI), Internet of Things (IoT) and using big data everywhere. All this new technology has totally changed how Indian society works, like entire industries and government organisations, even the ordinary citizens' daily lives. But there's downsides too, especially around the privacy of personal information of the people. This paper really dives deep into how all these emerging technologies clash with keeping data private in India. It takes a close look at the advantages and disadvantages of innovations like AI, including how helpful they can be but also how they could let personal information get exploited. A big focus is on how much these technologies rely on collecting tons of private data about people, analysing it and using it in ways individuals don't always agree to or even realise. This study was conducted using an empirical research method. Convenient sampling method was used to collect the samples and the sample size was 200. The sampling frame was set within Chennai, Tamil Nadu. The dependent variables are level of awareness about the emerging technologies, concerns regarding data privacy when using or interacting with emerging technologies, need for specific laws or regulations in India to address data privacy concerns related to emerging technologies, measures should be taken by the companies or organisations to ensure better data privacy protection, improvements or recommendations that would enhance data privacy in the context of emerging technologies in India and the independent variables are age, gender, educational qualification, salary and occupation. The research tools used here are bar charts for data analysis. On top of that, the paper really criticises India's current laws about data privacy, questioning if they can truly protect sensitive data from misuse and access by companies and governments, adopting more technologies. It points out the gaps and limitations in today's policies compared to global standards, and recommends India to update its rules to reduce privacy risks as much as possible while still encouraging innovation.

KEYWORDS: Artificial Intelligence (AI),Cybersecurity, Data privacy, Internet of Things (IoT), Security protocols and encryption.

INTRODUCTION

Nowadays, technology is evolving super quick and everything's connected globally. This has totally changed how societies work across the world. India is also seeing huge technological advancements lately in all types of areas. From everyone having smartphones to AI technologies in normal apps, India's really jumping on board the latest innovations. But with all these new technologies entering people's lives, data privacy becomes a big concern and as technology gets used more in everything we do, personal data collection, processing and use is everywhere. So while technological advancements bless us with some well advanced things in our lives, it also creates challenges around preserving sensitive information and data privacy rights. Especially with how digital India's population is growing, balancing new technology with proper data privacy protection is tricky. With the explosion in internet users, digital payments and online services, addressing these privacy concerns is crucial. So when innovative technology intersects with vital data protection needs, navigating towards robust frameworks is key. The data privacy issues presented by the emerging technologies are analysed in this paper. In addition it considers aspects of machine learning, blockchain big data analytics in relation to their connections to privacy rights. This research also considers regulations governing how data protection takes place in India. It seeks to unravel the complexities involving the attributes and influences of data privacy problems surrounding India's technology-based industry. Having a full control on these challenges is so important for authorities who make laws, companies, and even regular citizens since it allows everyone to make informed choices that find a good balance between using new technologies and upholding strong privacy standards. This paper encompasses ideas that contribute to the ongoing discussion on how India can effectively move forward with all these emerging technologies while still protecting people's privacy rights in an increasingly digital world. Technology has dramatically reshaped societies all over the world . The recent developments in technology in India over the years include IoT, artificial intelligence, and biometrics. Despite this, the emergence of modern technology and subsequent advances have led to fears surrounding individual digital privacy rights. The privacy and data protection framework in India has drawn criticism, and there is currently no specific data protection law in India. The Information Technology Act 2000, which was created before the spread of contemporary technologies, provides limited statutory protections and judicial rulings serve as an indirect kind of privacy protection. The Personal Data Protection Bill, 2019, which would create the first cross-sectoral legal framework for data protection in India, is currently under review. This paper looks into those questions - how developing technologies in India might affect privacy, what kind of laws or regulations could be put in place around using private data and how to make sure ethics are part of the conversation. The ultimate goal is to understand the realm of technologies and provide a good balance between taking advantage of new innovations while respecting the people's private information and data.

Digital Personal Data Protection Act (DPDPA) 2023:

The Digital Personal Data Protection Act (DPDPA) is an Indian law designed to protect the privacy of personal data in digital space. It includes the processing of personal data obtained in India, especially processed digitally and often goes further to include all activities outside Indian territory which have a direct or indirect link with offering goods or services within India. Some of the most attractive features of DPDPA include stimulating growth and innovation, splitting liability for organisations, as well as methods of governing data processors. But its implementation is not without difficulties. The concept of "deemed consent" is introduced by the law In some situations, people 'silence or inaction may be assumed to mean their consent. Personal data processed for personal or domestic purposes are exempted from the DPDPA. The Act also provides for progressive implementation, and organisations are authorised a reasonable period of time in which to make necessary preparations so as not to squander resources required in complying with the law. The DPDPA in particular represents progress towards securing data security under the new information age. At the same time it imposes on them the need to adjust their collection and usage procedures so as not fall foul of its stipulations.

AIM: To study the emerging technologies and data privacy challenges in India.

OBJECTIVES

- To examine the respondents' concerns regarding data privacy with emerging technologies.

- To analyse the measures should be taken by the companies or organisations to ensure better data privacy protection.
- To explore the improvements or recommendations that would enhance data privacy in the context of emerging technologies in India.

LITERATURE REVIEW

This paper examines how blockchain and AI could maybe work together to keep personal information safe. It talks about things like access control, protecting data, network security, and scaling - the main ways they could team up for privacy. Based on how blockchain and AI are used and built it puts strategies for privacy protection into categories and describes them. Trying to make a better base for guarding privacy, it finishes by proposing new solutions that would combine blockchain with AI to make things more efficient and secure **(Li Zongwei, 2023).** This paper is about the privacy questions with big data tech and it gives some ways to keep private information safe and suggestions for security processes for large data sets. It specifically deals with the ideas to have better privacy protection where blockchain and data science impact big data. In conclusion, it has recommendations for keeping personal information private in big data cases **(Kapil Joshi, 2023).** This article explores the ideologies of Internet of Things (IoT) hardware and software. It also examines how smart technologies like edge computing, 5G, and AI could shape the arena of future emerging technology. Besides peeking into the future it is important to delve into the real-world IoT apps like smart cities, transportation, healthcare, and farming **(Hudson Lubinga Nandere, 2023)**. This article examines the privacy issues that are connected with AI in the metaverse and possible attacks on privacy that could happen. The author came up with a new kind of attack that combines membership inference and reconstructed attacks to go after metaverse users. There are also some ideas for how to handle these problems that were identified **(Chamara Sandeepa, 2023)**. Making the metaverse raises questions about user privacy and protecting people's data. This article, for example, looks at important things like managing identities, authentication, securing information, and governance. It surveys these risks using promising technologies like hardware security cryptography and decentralised protocols carefully. Based on evaluating identities, data and threats the author suggests a framework that balances privacy, security, and ease of use. The solutions being used now will decide what the future decentralised and open metaverse might end up looking like **(Faramarz Zareian, 2023)**. This paper talks about the most interesting modern cybersecurity trends and how they could impact defending cyberspace in the future. The aim is to give institution policy makers, and other stakeholders some ideas and strategies to strengthen their cybersecurity protection. It does this by closely examining the challenges and opportunities related to these technologies **(Harshada Umesh Salvi, 2023)**. This paper tried to analyse the reasons for people's trust in new technologies more than traditional ones. It undermines how protecting personal information relates to trusting emerging technologies **(Mazey 2018)**. This paper is basically a how-to guide for protecting data privacy. It looks at different methods, both new and old, for keeping information confidential as people build digital systems to store assets like genomic data. The main suggestion is to combine traditional privacy approaches with some new technology to audit data transactions. The paper concludes that this could lead to new benefits which haven't been predicted yet, helping to ensure end users' privacy needs **(Jillian Mascelli 2023).** There's growing concern about securing individuals' genomic and health information. The usual ways of safeguarding privacy are getting limited, while new privacy-protecting technologies could let us share data more broadly for research **(Bonnie Berger, 2019).** The paper argues that there is a need to rethink privacy given how much modern life depends on information networks now. The whole concept and related laws come from a different era. The values matter as much as ever, but privacy itself is evolving. We have to update how we protect it. The author makes the case for a more ethical approach to privacy impact assessment **(Friedewald et al. 2010).** A section in Science and Public Policy talks about how fast science and technology moves compared to things like human rights and privacy. The authors want to find new ways for global leaders to deal with these challenges better **(Friedewald, 2013).** The author explains that people care about more than just blindly trusting and getting excited about new technology is what they think makes up a healthy society. The "Privacy Paradox" says that new technology tends to make people not pay attention as much to potential ethical issues and privacy problems with data, which can violate privacy of personal information. So this research shows that people's desire to have the newest technology can lower their moral values, compromising on privacy **(Adil Bilal, 2022).** This paper examines the crucial aspects of cybersecurity, including why it matters, new emerging technologies, management rules and regulations, risks from suppliers and what might happen in the future. It further explains how important it is to

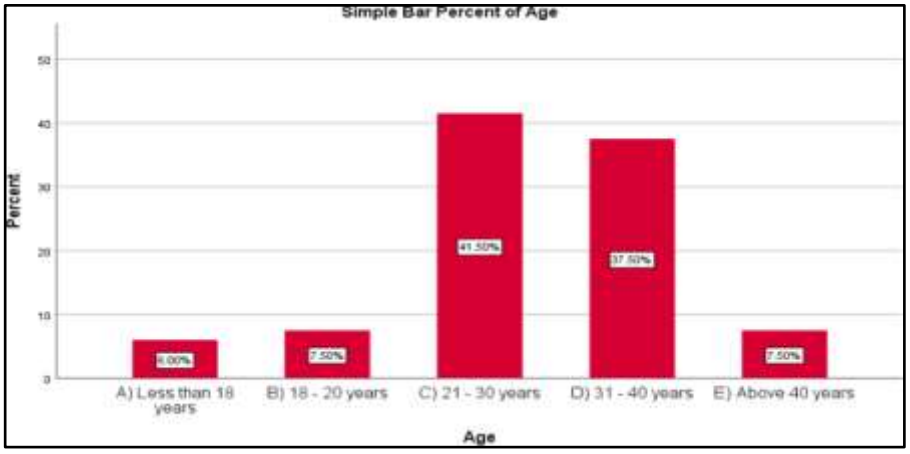
think about risks and to get people on board with caring about cybersecurity **(Deepak Kumar Mandal, 2023).** This paper takes a careful look at the 2019 draft law. It tries to compare the Data Protection Impact Assessment (DPAI) with the EuropeanData Protection Board (EDPB) and the General Data Protection Regulation (GDPR). It also looks at how the DPAI matches up to other laws already in place in India and the paper talks about how Indian courts have seen privacy and defined it within the Indian constitution. The paper discusses the rights part of the 2019 Bill which also points out possible trouble for the right to privacy that might come from the newer 2021 Bill **(Sharma, Aana 2023).** This paper aims to reveal the challenges faced by internet users regarding data security, privacy and safety in a world where they entrust their private personal information to corporations. For computer and smartphone users they have some concerns including insecure data sharing, data breaches, inability to protect personal information, companies selling data to third parties, and weak online platform security. The rise in concerns among varying Indian user groups and proposed policy measures, particularly on privacy, data protection and security, are discussed as such data must be safeguarded for consumer's welfare **(Arokiaraj David 2023)**. This paper examines the current data privacy debates in India and the European Union. Its goal is to analyse data privacy and protection issues rising from technological developments in these countries that shape modern trends. The paper also briefly analyses various data privacy laws, new developments, loopholes in applicable laws, and inconsistencies between the two regimes **(Priyamvada Pandey 2023).** This paper analyses the Indian citizen's views about digital privacy rules. Keeping personal information private is a big deal nowadays when everybody's information, financial data, and other basic information are online and in need of protection. Thus it shows that people, companies and the government have to be careful with these technologies and set up shields to keep data safe **(Swain et al, 2023).** The goal here is to check out the duties social media sites have to undertake with respect to people's privacy and guard their information. The author compares privacy laws across the world - the US, UK, France, Germany - with a focus on India's rules. India's Information Technology Act was meant to grow online business, but it also raises privacy issues. Having strong data protection is key, and India doesn't completely have that yet. This paper also talks about how much responsibility intermediaries have to keep data safe, looking at how it works in different countries and India as they deal with critical cyber security problems **(Prasun Singh 2022).** The AIs future seems good yet concerning as the advanced technological developments grow more complex for creators as well as the users. There's a lot to unwrap here - from AI's brief history to problems still needing solutions today, not to mention dealing with biases and privacy issues that undermine public trust. This paper contextualising these challenges is key, as is proposing solutions during AI's advancement to tackle lingering hurdles and emerging wireless networks offer continuous convenient communication without much equipment. Fueled by things like the Internet, blockchain, cloud computing and big data, they transport more sensitive information than ever **(Annie Benzie 2023).** This paper addresses the security and privacy issues - from network access and authentication to protecting user data. Though research continues, investigations into these persistent problems, there is an urgent need for secure data transactions. New schemes also introduce other concerns around accessing networks and preserving privacy that require attention as reliance on wireless technology increases (Xiaodong Lin 2020).

METHODOLOGY:

Empirical research method was used in this study. The sampling method taken here was the convenient sampling method and the sample size was 200. The sampling frame was set within Chennai, Tamil Nadu. The dependent variables are level of awareness about the emerging technologies, concerns regarding data privacy when using or interacting with emerging technologies, need for specific laws or regulations in India to address data privacy concerns related to emerging technologies, measures should be taken by the companies or organisations to ensure better data privacy protection, improvements or recommendations that would enhance data privacy in the context of emerging technologies in India and the independent variables are age, gender, educational qualification, salary and occupation. The research tools used here are bar charts for data analysis.

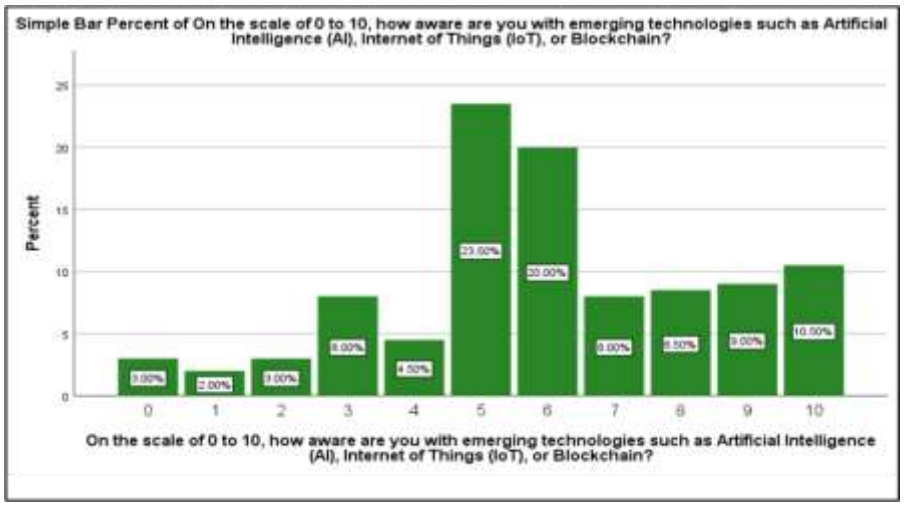
ANALYSIS:

FIGURE 1



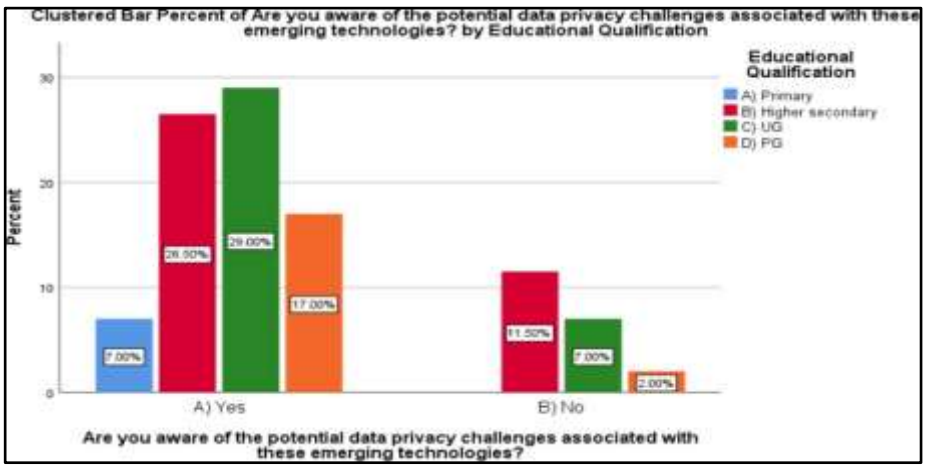
LEGEND: Figure 1 presents the distribution of ages among the individuals who participated in the survey.

FIGURE 2



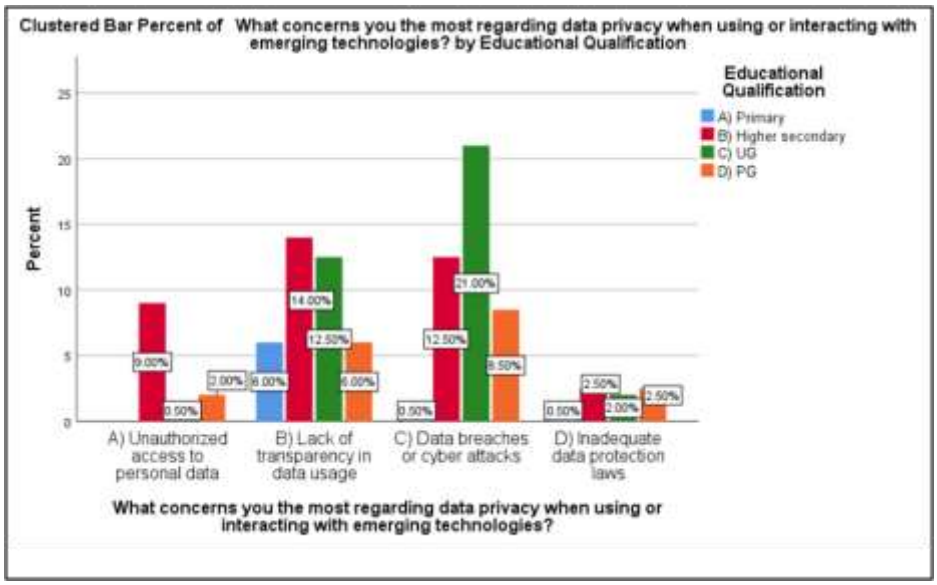
LEGEND: Figure 2, shows the survey respondents' level of awareness about the emerging technologies such as Artificial Intelligence (AI), Internet of Things (IoT) or Blockchain.

FIGURE 3



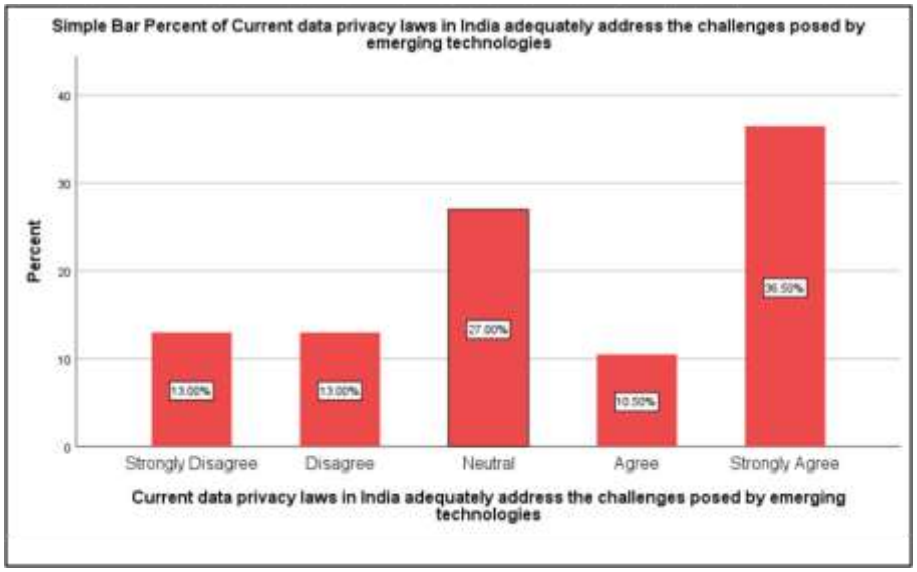
LEGEND: Figure 3, shows whether the survey respondents are aware about the potential data privacy challenges associated with the emerging technologies with educational qualifications.

FIGURE 4



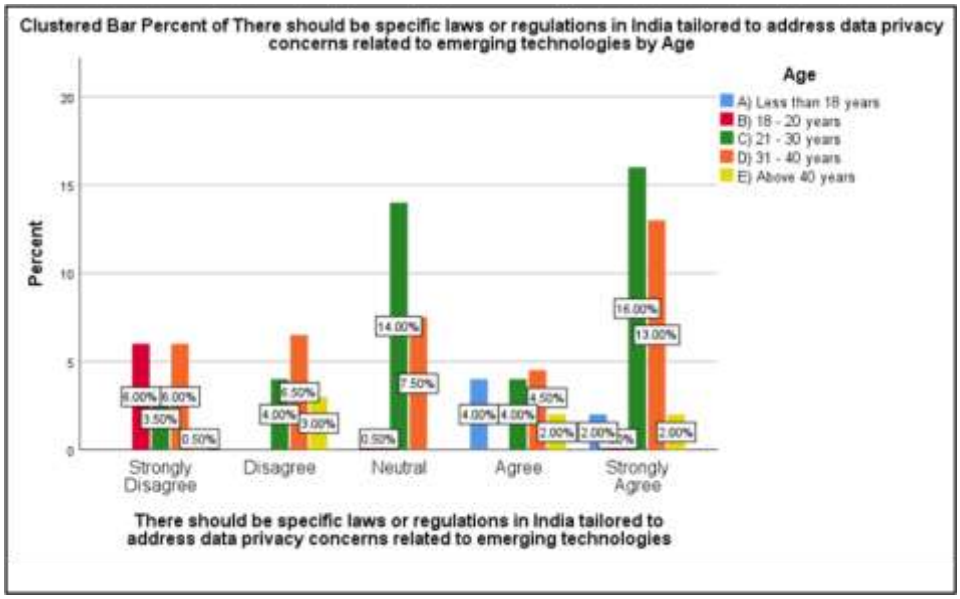
LEGEND: Figure 4, shows the respondents' concerns regarding data privacy when using or interacting with emerging technologies.

FIGURE 5



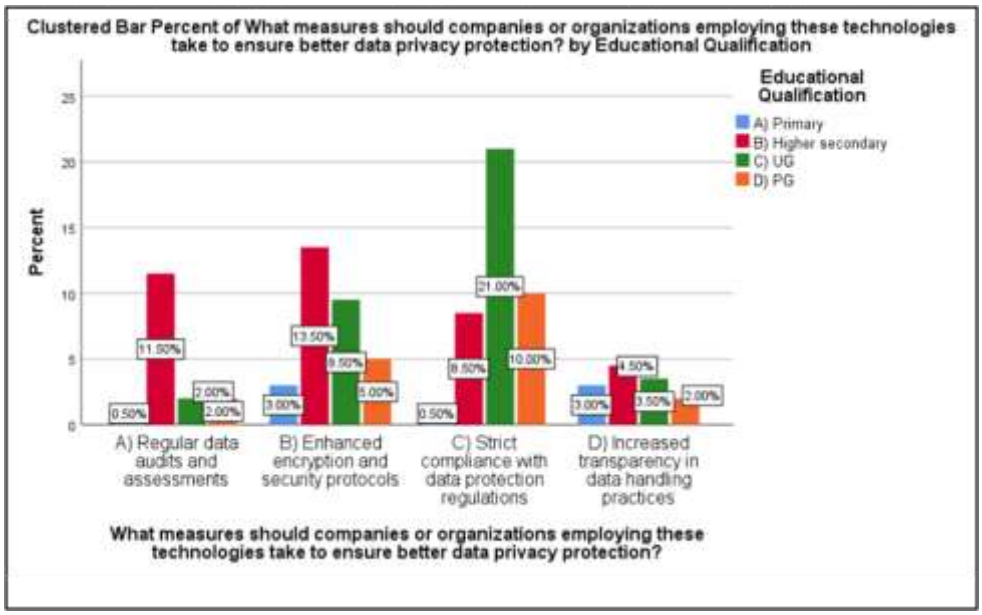
LEGEND: Figure 5, shows the opinions of survey respondents whether the current data privacy laws in India adequately address the challenges posed by emerging technologies.

FIGURE 6



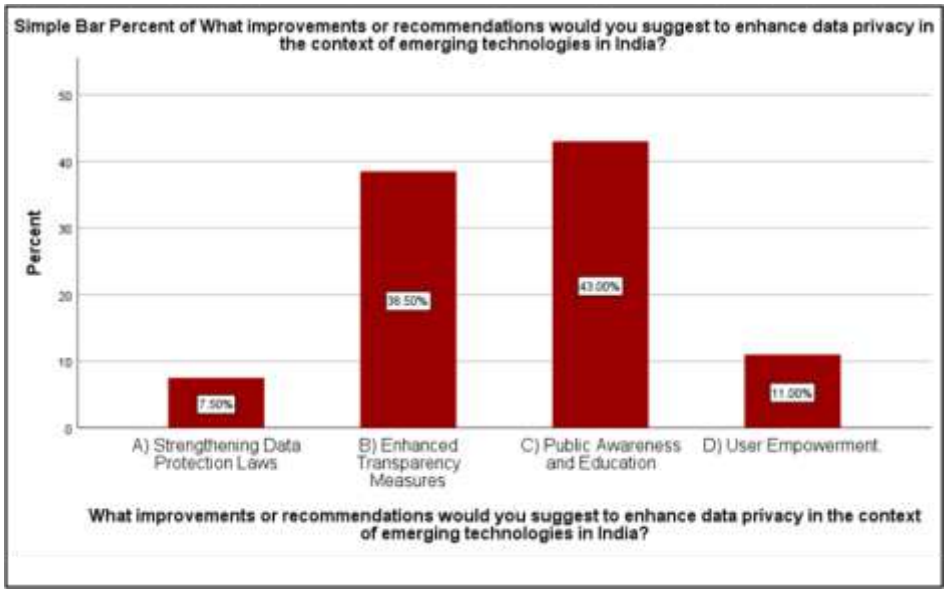
LEGEND: Figure 6, shows the opinion of survey respondents on whether there should be specific laws or regulations in India tailored to address data privacy concerns related to emerging technologies.

FIGURE 7



LEGEND: Figure 7, shows the opinions of survey respondents on the measures should be taken by the companies or organisations while employing these technologies to ensure better data privacy protection.

FIGURE 8



LEGEND: Figure 8, shows the opinion of survey respondents on the improvements or recommendations that would enhance data privacy in the context of emerging technologies in India.

RESULT

In **figure 1**, survey respondents belonging to the age group of 31- 50 years are high with 41.50% followed by 31-40 years (37.5%). In **figure 2**, survey respondents aren't much aware about the emerging technologies such as Artificial Intelligence (AI), Internet of Things (IoT) or Blockchain. In **figure 3**, more than 65% of survey respondents are aware of potential data privacy challenges associated with the emerging technologies. In **figure 4**, more than 40% of survey respondents have opined that data breaches or cyber attacks, concerns them the most regarding data privacy when using or interacting with these emerging technologies. In **figure 5,** more than 45% of survey respondents have agreed that the current data privacy laws in India adequately address the challenges posed by emerging technologies. In **figure 6**, while comparing the opinions with the age of the respondents, more than 40% have agreed that there should be specific laws or regulations in India tailored to address data privacy concerns related to emerging technologies. In **figure 7**, while comparing the opinions with the educational qualifications of the respondents, 40% of survey respondents have opined that the strict compliance with data protection regulations should be the primary measures taken by the companies or organisations while employing these technologies to ensure better data privacy protection followed by enhanced encryption and security protocols (31%). In **figure 8**, survey respondents have opined that public awareness and education (43%) could be the major improvements or recommendations that would enhance data privacy in the context of emerging technologies in India followed by enhanced transparency measures (38.5%).

DISCUSSION

It can be seen that survey respondents aren't much aware about the emerging technologies such as Artificial Intelligence (AI), Internet of Things (IoT) or Blockchain. The lack of awareness about emerging technologies like Artificial Intelligence (AI), Internet of Things (IoT, and Blockchain among survey respondents can be attributed to several factors. There could be factors contributing to this situation. Firstly the intricate nature of these technologies might pose a challenge for the public to grasp their applications and implications. Moreover, given the pace at which technology evolves, it's possible that there is a time gap in knowledge as these advancements continue. Additionally, how information about these technologies is conveyed to the public may also influence their awareness. For instance if the information is presented using terms or jargon it could contribute to a lack of understanding.Addressing this issue may require efforts to improve the accessibility of information about these technologies through education, public engagement, and clear communication strategies **(Figure 2).** It can be seen that more than 65% of the individuals surveyed expressed their concerns about the potential privacy issues associated with the increasing use of new technologies like AI, IoT and blockchain. This provides further concerns over the issue of data privacy as the use of

social media and digitization intensifies. People are worried about how AI systems, which heavily rely on comprehensive data, can expose sensitive information or perpetuate biases. Similarly the growing number of technologies raises concerns about the collection and sharing of data without proper user consent. Additionally while blockchain technology is known for its security features it also contains privacy challenges since transactions can be traced back potentially revealing details. The prevalence of data breaches and heightened consumers' unease regarding data privacy further emphasise the need for comprehensive privacy regulations and collaborative efforts, among policymakers, technology developers and legal experts to address these challenges and protect individuals privacy as technology continues to advance **(Figure 3).** According to the survey, more than 40% of respondents are concerned about data breaches or cyber attacks when using or interacting with emerging technologies. This is a significant concern as personal data are more exposed than ever in the evolving emerging technology landscape but are often insufficiently protected from being stolen, copied, transmitted, viewed, or used by an unauthorised individual. Data breaches can be costly, with the average cost being USD 392 million. Credentials being stolen contribute to nearly 63% of the data breaches, and insider threats and an overreliance on third-party vendors are also alarming trends. It is crucial to think about innovative approaches to resolve these concerns rather than relying on subjective analysis, bias, and limited data sets. It also indicates that emerging technology is more prone to attacks, and data-privacy technology will need to mature quickly to effectively manage today's endlessly growing data wave **(Figure 4).** More than 45% of survey respondents have agreed that the current data privacy laws in India adequately address the challenges posed by emerging technologies. India has recently passed a law called the Digital Personal Data Protection Act, which will replace provisions of the Information Technology Act. This new law sets guidelines for how organisations should handle data and aims to address privacy concerns associated with advancements. Under this law entities collecting user data will be required to obtain user consent. In addition specific entities will be designated as "Significant Data Fiduciaries," and penalties of up to 250 crore rupees (million) can be imposed for noncompliance. This is a step towards ensuring privacy protection especially as technologies continue to evolve. However it is crucial to monitor the effectiveness of this law in dealing with challenges posed by emerging technologies and ensure that it keeps up with advancements considering consumer trends and global privacy protection measures, across all businesses **(Figure 5).** It can be seen that more than 40% of respondents believe that specific laws or regulations should be implemented in India to address data privacy concerns related to emerging technologies. This is, in line with the approval of the Digital Personal Data Protection Act, which seeks to create a framework for safeguarding data. It defines guidelines and rules for how data should be handled and deals with consent requirements and individual rights relating to storage of information. This Act mandates every organisation and institutions that collect user data to obtain consent from users with an exception. Additionally it places responsibilities on those who control the data. As such emerging trends, such as AI, Internet-of-things (IoT) and blockchain raise questions regarding information confidentiality, the significance of enacting privacy rules takes greater relevance. With India having over 750 million active internet users, this Act's impact could encompass all areas **(Figure 6)**. It can be seen that 40% of survey respondents believe that strict compliance with data protection regulations should be the primary measure taken by companies to ensure better data privacy protection. The latest India's Digital Personal Data Protection Act of 2023 (DPDPA) is only one in line with the general world trend for tighter control over personal information and other data management issues. More than one-hundred countries already have implemented privacy legislations and data breaches, with a growing interest in protecting personal private information, companies should take necessary steps in this regard. This aligns with the sentiments of 40% of survey respondents who believe that strict compliance with data protection regulations should be the primary measure taken by companies to ensure better data privacy protection, followed by enhanced encryption and security protocols at 31%. The DPDPA which was designed in the mode of EU's General Data Protection Regulation (GDPR) stresses the significance of enhanced data protection legislation along with improved encryption and protective measures. Such laws passing, as well as evolving international regulatory landscape means that more attention needs to be focused on data security before deploying the technologies dealing with personal data **(Figure 7).** It can be seen that 43% of respondents believe that improved public awareness and education would be the major improvements or recommendations to enhance data privacy. This is followed by enhanced transparency measures, which 38.5% of respondents consider important. The results indicate the necessity of totaling privacy standards along with strong legislation to tackle the threats of new technological innovations like artificial intelligence, face recognition, and biometrics. Indian Supreme court has recognized the constitutional status of privacy which is a fundamental right and recently enacted Digital Personal Data Protection Act (DPDPA) provides for a legal framework of data protection.

However, there is still significant progress needed on the data privacy front, in that data economics do not adequately address harm-privacy related today. Therefore, it is incumbent upon policy makers, technologists, and legal experts to work together towards developing appropriate data protection laws that will ensure privacy while at the same time promoting the development and growth of the economy **(Figure 8)**.

LIMITATIONS:

As the research is directed towards the selection of in-depth inquiry of specific settings infused with values, beliefs, perception, politics, ideology and the lack of government initiatives might diminish the researcher's analytical objectivity and independence of the research.

SUGGESTION:

Modern technologies like Artificial Intelligence (AI) and the Internet of Things (IoT) are changing the way our information is being used in India. It's important to understand these technologies in order to make sure our personal information stays safe. People should check if the rules that are used to protect our information are good enough for these new technological changes and think about making them better if needed. When creating these new technologies, there is a need to think about privacy right from the beginning. It is also a good idea to keep our information safe by knowing our rights about privacy. It's not just about one group; we should all work together - the government, companies, and the citizens to make better rules and protect our information. Some new technological ideas, like using special codes or encryption, might help too. Lastly, it's important to think about what might happen in the future with our privacy and these new technologies. By planning now, we can keep our information safe in the changing world of technology.

CONCLUSION

Rapid technological advancement in India has opened doors, but also complex privacy challenges. As innovation marches on, safeguarding personal data grows more vital yet tricky and India's exploding technology sector and digital makeover spark thorny data privacy issues. The emerging role of AI, big data analytics, the Internet of Things (IoT) and other emerging tech concerns the need for strong data protection actions. While India's taken constructive steps around data privacy regulations, practical problems around implementation and enforcement still remains. Policymakers, companies and people walk a tightrope balancing innovation and privacy. It's important that the government, businesses and citizens team up addressing these challenges. Educating people on data rights, instilling accountable data handling practices in companies, and refining legal guardrails can steer India toward a more secure, privacy-focused tech landscape. As India's technology continues transforming, data privacy must stay a top priority. There is a need to strike the right balance between fostering innovation and safeguarding personal privacy as it will be vital for the country's digital ecosystem's sustainable evolution.

REFERENCES

1. Bonnie Berger in Emerging technologies towards enhancing privacy in genomic data sharing, December 2019, Genome Biology 20(1), DOI:10.1186/s13059-019-1741-0, Massachusetts Institute of Technology
2. Jillian Mascelli in Data Privacy for Digital Asset Systems, September 2023, Finance and Economics Discussion Series, DOI:10.17016/FEDS.2023.059
3. Michael Friedewald in Privacy, data protection and emerging sciences and technologies: Towards a common framework, Innovation - The European Journal of Social Science Research Vol. 23, No. 1, March 2010, 6167. doi:10.1080/13511611003791184.
4. Michael Friedewald in To special section: Governing privacy and data protection issues of emerging technologies, December 2013, Science and Public Policy 40(6):705-707, DOI:10.1093/scipol/sct094.

5. Adil Bilal in Rise of Technomoral Virtues for Artificial Intelligence-based Emerging Technologies' Users and Producers: Threats to Personal Information Privacy, the Privacy Paradox, Trust in Emerging Technologies, and Virtue Ethics, February 2022, DOI:10.13140/RG.2.2.23285.04327, Thesis for: Doctor of Philosophy in Information Systems, University of Canterbury
6. Deepak Kumar Mandal in Cybersecurity in the Era of Emerging Technology, June 2023, In book: Emerging Technology and Management Trends (pp.108-134), IIMT Group of Colleges
7. Zongwei Li, Dechao Kong, Yuanzheng Niu, Hongli Peng in An Overview of AI and Blockchain Integration for Privacy-Preserving, May 2023
8. Kapil Joshi in Right to Digital Privacy: A Technological Intervention of Blockchain and Big Data Analytics, April 2023, Conference: 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttaranchal University
9. Hudson Lubinga Nandere in Emerging Technologies and Applications of IoT: Current and Future Perspectives, October 2023, International Journal of Innovative Science and Research Technology 8(10):151-160, Bugema University (BU)
10. Chamara Sandeepa in Privacy of the Metaverse: Current Issues, AI Attacks, and Possible Solutions, June 2023, DOI:10.1109/MetaCom57706.2023.00052, Conference: IEEE International Conference on Metaverse Computing, Networking and Applications (IEEE MetaCom 2023), University College Dublin
11. Faramarz Zareian in Privacy and Security Challenges in the Emerging Metaverse, August 2023, DOI:10.13140/RG.2.2.22144.40964, Università degli Studi di Genova
12. Harshada Umesh Salvi in Emerging Trends and Future Prospects of Cybersecurity Technologies: Addressing Challenges and Opportunities, August 2023, International Journal of Scientific Research in Science and Technology, DOI:10.32628/IJSRST52310432
13. Annie Benzie in Bias, Privacy and Mistrust: Considering the Ethical Challenges of Artificial Intelligence, September 2023, DOI:10.1007/978-3-031-40118-3_1, In book: Applications for Artificial Intelligence and Digital Forensics in National Security (pp.1-14)
14. Xiaodong Lin, Mohsen Guizani, Xiaojiang Du, Cheng-Kang Chu in Advances of Security and Privacy Techniques in Emerging Wireless Networks, June 2020, IEEE Wireless Communications 27(3):8-9, DOI:10.1109/MWC.2020.9116080
15. Mazey, Natasha in Initial trust in emerging technologies and the effect of threats to privacy, 2018, http://dx.doi.org/10.26021/5330.
16. Arokiaraj David, Jeganathan Gomathi Sankar in Internet Users Top Concerns Ensuring Data Privacy, Security, and Protection, May 2023, Conference: 10th International Conference on Multidisciplinary Research and Modern Education
17. Priyamvada Pandey in A Critical Analysis of Data Privacy and Issues in Contemporary Indo-European Context, January 2023, In book: Institutions, Practice and Digital Transformation in India and Europe (pp.63-74), Edition: 2023, Chapter: 6, University of Delhi
18. Swain, Prakash & Kumar, Anil & Gadgil, Prof & Srivastava, Dr & Swain, Dr & Sahu, Shekhar in An Analysis Of The Laws Concerning Digital Privacy, February (2023), Russian Law Journal. 9. 270-277
19. Prasun Singh in Privacy and Data Protection in Social Media and Liabilities of Intermediaries, January 2022, DOI:10.55662/book.2022CCRS.010, In book: Cyber Crime, Regulations and Security - Contemporary Issues and Challenges (pp.198-214), Sharda University.
20. Aana Sharma in Data Protection, Privacy and Proposed Law in India: Tracing the Previous Challenges and Transition to the Bill of 2021, Volume II 2021 HPNLU Law Journal, 31 March 2023, National Law Institute University (NLIU); Himachal Pradesh National Law University