ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

OPEN ACCESS Original Research Article

STUDY ON DATA BROKERS AND THEIR IMPACT ON CYBERSECURITY THREATS IN INDIA

*** Adarsh Santosh Nair, ** Deepakkrishnan Balkrishnan Nair, *** Shreeya Nitin Palkar & **** Mrs. Komal Tiwari

*Research Students, ****Research Guide, B. K. Birla College, Kalyan.

Abstract:

This study explores the role of data brokers in shaping cybersecurity threats within the context of India's digital development, a critical yet under-researched topic in the era of digital connectivity. While data brokers operate in regulated sectors and facilitate economic and technological growth by aggregating and distributing personal data, their unregulated activities can also expose individuals and organizations to significant cybersecurity risks, such as identity theft, fraud, Scams and data breaches. The research investigates the level of concern regarding personal data collection across different age groups. The findings reveal that younger individuals are more aware of the risks associated with data collection, while older demographics exhibit lower levels of concern, highlighting the need for tailored awareness campaigns. Additionally, the research establishes a significant connection between the operations of data brokers and the increasing frequency of cybersecurity threats, such as identity theft and fraud. The study underscores the urgent need for stricter regulations, enhanced transparency in data collection practices, and robust cybersecurity measures. It concludes with recommendations for policymakers and organizations to adopt data protection frameworks, educate vulnerable groups, and collaborate to create a safer digital ecosystem in India.

Keywords: *Data brokers, Cybersecurity threats, India, Digital development, Personal data, Identity theft, Fraud, Scams, Data breaches, Unregulated activities, Awareness campaigns, Transparency, Data collection, Regulations, Data protection frameworks, Digital ecosystem.*

Introduction:

A data broker is an entity that collects personal information about individuals from public and sometimes private sources, then sells or licenses this data to third parties. Known as information brokers, they include companies like Experian and Equifax. Globally, many data brokerages earn significant revenue by sharing personal information, with similar operations in India. Indian data brokers gather data from public records, online activities, and surveys.

They function under regulations like the IT Act and the Digital Personal Data Protection Act, but numerous unregulated sectors raise cybersecurity concerns.

In the first four months of 2024, the Indian Cyber Crime Coordination Centre (I4C) recorded over 7.4 lakh cybercrime incidents, with cyber fraud losses amounting to ₹11,333 crore in the first nine months. Currently, the most successful scam that individuals are falling for are "Digital Arrest" scam, where scammers impersonate as police officials and extort large amount of cash out of their victims as "Bail money". A significant issue in India is the unauthorized trade of personal data by data brokers to fraudsters, who often buy this information for as little as ₹150 to ₹300. Data brokers collect personal data without consent, making it easy for scammers to target individuals. They often exploit vulnerable populations, especially the elderly, using personal details to conduct scams. In response, India has implemented the Digital Personal Data Protection Act, aiming for compliance in two to three

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

OPEN ACCESS Original Research Article

years.

Research on data brokers is crucial because they collect and sell personal information, often without people's knowledge, creating opportunities for fraud. This is especially concerning in India, where digital technology is growing faster than awareness of data privacy. Scammers use this data to carry out targeted attacks. Studies can help identify the most misused types of data and how scammers obtain them, leading to better prevention strategies. While the Digital Personal Data Protection Act (DPDPA, 2023) aims to curb misuse, its enforcement is still in the early stages. Research is needed to assess the law's impact, hold data brokers accountable, and protect vulnerable individuals from scams.

Review of Literature:

In his study, **"Cyber Security and Data Protection: Challenges in the Indian Context**," **Subhasis Das** highlights concerns about India's digital growth, noting that progress appears more accidental than planned. A Facebook data breach recently affected about 562,000 users in India—a smaller number compared to 87 million in the U.S. and 1 million in the U.K.—but still significant. While allegations of election manipulation in India lack clear evidence, the limited focus on social media marketing by internet companies has helped reduce negative impacts. Das views Christopher Wylie's revelations as a timely warning about the risks of data

breaches, especially as India's digital and data use is poised for rapid growth. He stresses the importance of raising awareness among lawmakers, experts, and citizens to ensure a safer and more secure digital future for the country. **(Das, 2018)**

"**Privacy, Data Protection, and Cyber Security in India**", a research paper by **Nishith Desai Associates**, highlights that cybersecurity is a major concern for national security in India. Even with rules in place, over 1.4 million cybersecurity incidents were reported in 2021, showing that the current system needs improvement. The paper discusses new guidelines aimed at making industries more active in reporting and following cybersecurity rules. It also talks about the government's efforts to protect consumer data and give authorities access to data for enforcement, especially in industries like telecom, banking, and insurance. While these guidelines are important for creating a safer internet, some of the rules are still unclear, and it remains to be seen how they will be enforced. **(Aaron Kamath, Purushotham Kittane, Aniruddha Majumdar, Varsha Rajesh, 2023)**

"**Data Brokers in an Open Society**", an '**Upturn**' report for the '**Open Society Foundation**' by **Aaron Rieke**, **Harlan Yu**, **David Robinson**, and **Joris von Hoboken** discuss how data brokerage and profiling are becoming more important in decisions that affect people's rights around the world. They believe this trend will keep growing. They suggest that we should focus on cases where protecting privacy and other basic rights, like fairness and due process, are both important. By looking at these situations, they argue that we can push for stronger privacy rules while also working towards other important social justice goals. **(Aaron Rieke, Harlan Yu, David Robinson, Joris Von Hoboken, 2016)**

Hyeontaek Oh, **Sangdon Park**, **Gyu Myoung Lee**, **Hwanjo Heo**, and **Jun Kyun Choi** in their research paper "**Personal Data Trading Scheme for Data Brokers in IoT Data Marketplaces**", a new model for personal data trading is proposed. The model involves data providers, a data broker, and data consumers, and considers different types of personal data. The authors develop functions for data trading (WTS and WTB) to estimate the number of providers and consumers and create a model to assess data quality. Their approach finds the best solution for maximizing the data broker's profit and is suitable for current IoT

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

OPEN ACCESS Original Research Article

marketplaces. They also suggest adding multiple data stores, brokers, and cost models, along with using an auditable ledger for tracking personal data transactions in future work. **(Hyeontaek Oh, Sangdon Park, Gyu Myoung Lee, Hwanjo Heo, Jun kyun Choi, 2019)**

The research paper "**How Social Networks and Data Brokers Trade with Private Data**" by **Germán Llorca-Abad** and **Lorena Cano-Orón** explains how the data market is closely tied to the loss of users' privacy. The authors point out that current laws do not do enough to protect people's rights. They believe that improving digital literacy is essential. If people understand the importance of privacy and the value of their data, they can take better control of their personal information, which will help reduce the information gap. **(Germán Llorca-Abad, Lorena Cano-Orón, 2016)**

Research Methodology:

Research Questions:

This research seeks to investigate important inquiries regarding the function of data brokers and their influence on cybersecurity in India. It centers on exploring how data brokers gather, maintain, and distribute information, along with the cybersecurity threats linked to these activities. The study additionally explores the impact of data brokers on the safety of individuals and organizations. Furthermore, it examines the efficiency of the existing legal and regulatory framework for data brokers in India and proposes methods to mitigate the cybersecurity threats they present.

Objectives of the Research:

1. To comprehend how data brokers function in India.
2. To investigate the cybersecurity threats linked to data brokers.
3. To examine the legal structure governing data brokers in India.
4. To recommend actions to mitigate cybersecurity threats posed by data brokers. **Significance of the Research:**

This research is significant as it investigates the function of data brokers in India and their influence on cybersecurity. With the increasing utilization of personal and organizational data, it is essential to comprehend the functioning of data brokers. The study aids in recognizing the dangers they present to people and companies, increases awareness regarding these risks, and emphasizes the necessity for improved regulations. By tackling these challenges, the research seeks to enhance cybersecurity protocols and promote a more secure digital landscape in India.

Hypothesis:

Hypothesis 1: Level of concern about personal data being collected across different age groups -

- **Null Hypothesis (H_0):** There is no difference in the level of concern about personal data being collected across different age groups.
- **Alternative Hypothesis (H_1):** There is a significant difference in the level of concern about personal data being collected across different age groups.

Hypothesis 2: Data Brokers and their impact on cybersecurity in India -

- **Null Hypothesis (H_0)**: Data brokers do not have impact on the cybersecurity threats in India
- **Alternative Hypothesis (H_1):** Data brokers do have impact on the cybersecurity threats in India

Methodology:

This research utilizes a Qualitative Research framework to explore the function of data brokers and their influence on cybersecurity in India. The study mainly relies on Secondary Data, such as reports, scholarly articles, and research papers on cybersecurity and data brokers to gain insight into the activities of data brokers. The Purposive Sampling technique is employed to choose participants with knowledge or direct experience regarding data brokers and cybersecurity matters. The information is subsequently examined through Thematic Analysis to uncover

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

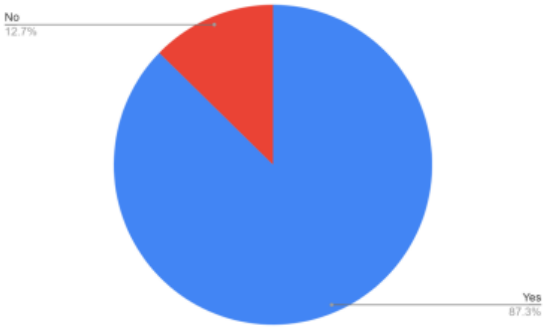
OPEN ACCESS Original Research Article

repetitive themes, risks, and patterns associated with data broker operations. Ethical protocols are adhered to during the research, guaranteeing informed consent and privacy for participants

Limitations of the Research: Although more than 70 participants were included, the study might still encounter difficulties in thoroughly representing the varied viewpoints on data brokers and cybersecurity from various sectors. Moreover, although secondary data offers important insights, it might be constrained in breadth or outdated, potentially affecting the depth and applicability of the results. Another constraint is the intrinsic challenge in acquiring comprehensive, direct insights into the activities of data brokers, due to the secretive and frequently unclear nature of their operations. Ultimately, the ever-changing characteristics of cybersecurity threats and data broker operations imply that the findings of the study could change as new advancements arise in the sector.

Data Analysis:

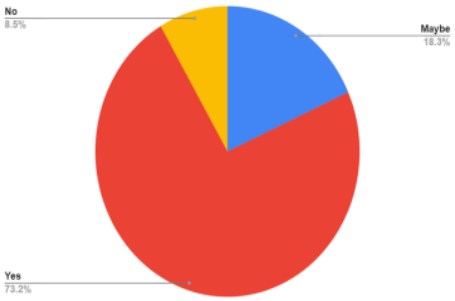
• Are you aware of the term "data brokers"?



Interpretation: From the data above, majority of our respondents are aware of the term "Data Brokers", being 87.3% of the respondents saying 'Yes'. Rest of the respondents were unaware, being 12.7% of the respondents being 'No'. The respondents who said 'Yes' also shared their source where they heard about 'Data Brokers':

- Newspapers / News article
- Social Media
- Professional Experience
- Friends and Family

• Do you think, data brokers collect and sell your personal information?



Interpretation: From the data above, majority of our respondents are aware or think that Data Brokers collect and sell their personal information, being 73.2% of the respondents saying 'Yes'. Others either aren't sure (18.3%) or disagree (8.5%)

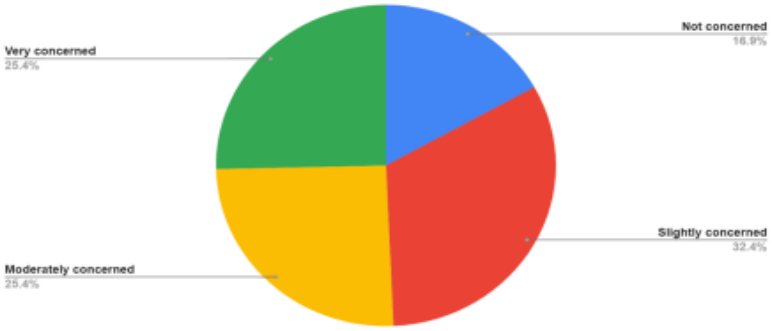
ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

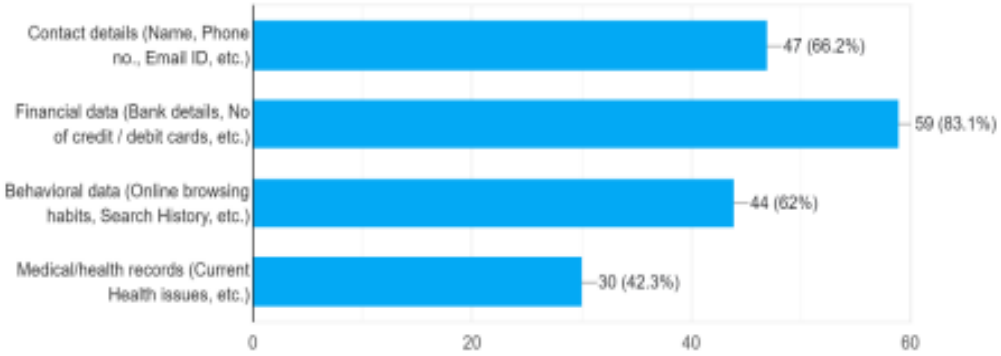
OPEN ACCESS Original Research Article

• How concerned are you about your personal data being collected without consent?



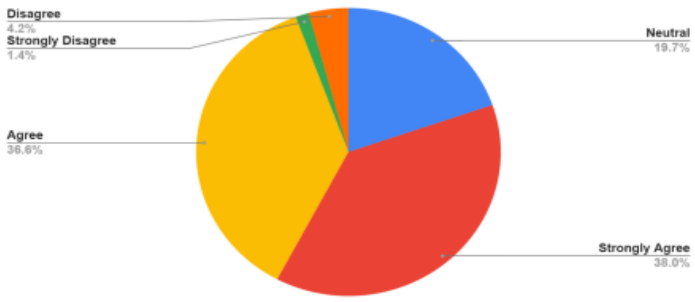
Interpretation: From the data above, we can see that our majority respondents are slightly concerned about their data being collected without their consent, being 32.4% of responses. Rest are either very or moderately concerned (25.4%) and not concerned at all (16.8%).

• In your opinion, which types of personal data do you believe are most at risk of being collected by data brokers?



Interpretation: From the data above, the most vulnerable data that data brokers have are Financial Data, being 83.1% of the respondents voting for the personal data that they believe is more at risk of being collected by data brokers. Rest being Contact Detail (66.2%), Behavioural Data (62%) and Medical records (42.3%).

• Do you believe data brokers contribute to cybercrimes, (Like the current "Digital Arrest" Scam, Call Center Scams, Fake Lottery winnings, Phishing mails etc.)



Interpretation: From the above data, it shows that 38.0% of respondents strongly agree, and 36.6% agree that data brokers contribute to cybercrimes like scams and phishing. 19.7% are neutral, while only 4.2% disagree and 1.4% strongly disagree.

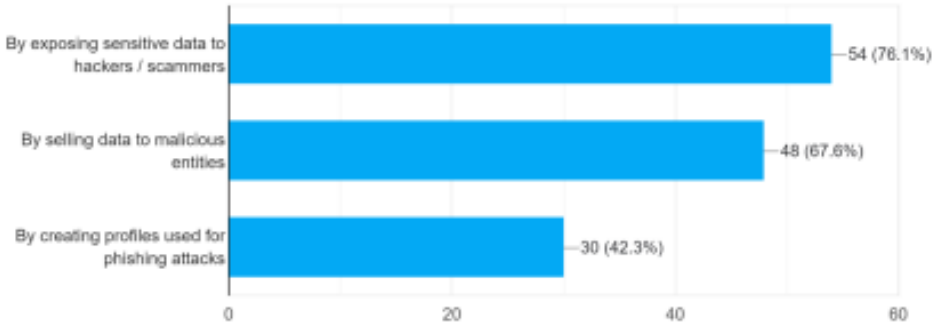
ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

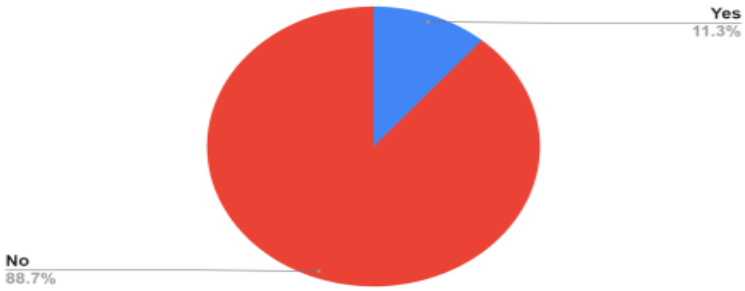
OPEN ACCESS Original Research Article

• In your opinion, how data brokers can increase cybersecurity risks for people in India?



Interpretation: From the data above, respondents say that data brokers can increase cybersecurity risk by exposing sensitive data to hackers / scammers, being 76.1% of the votes going to this option. Rest being by selling data to malicious entities (67.6%) and by creating profiles used for phishing attacks (42.3%).

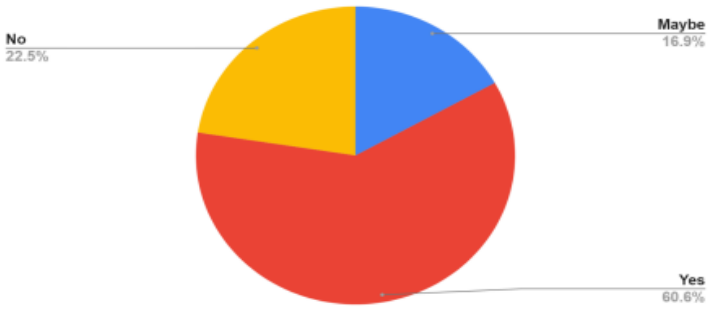
• Have you ever been a victim of a cybercrime? (Like the current "Digital Arrest" Scam, Call Center Scams, Fake Lottery winnings, Phishing mails etc.)



Interpretation: From the data above, 11.3% of our respondents were victims of a cybercrime and the rest were not (88.7%). 11.3% were open to share what cybercrime they became a victim to:

- Phishing mails
- Fake recharge scams
- UPI Frauds

• Are you aware of any laws in India that regulate the activities of data brokers?



Interpretation: From the data above, 60.6% of respondents agree stricter regulations are needed to monitor data brokers in India. 22.5% disagree, while 16.9% are unsure, indicating some lack of awareness or mixed opinions on the issue.

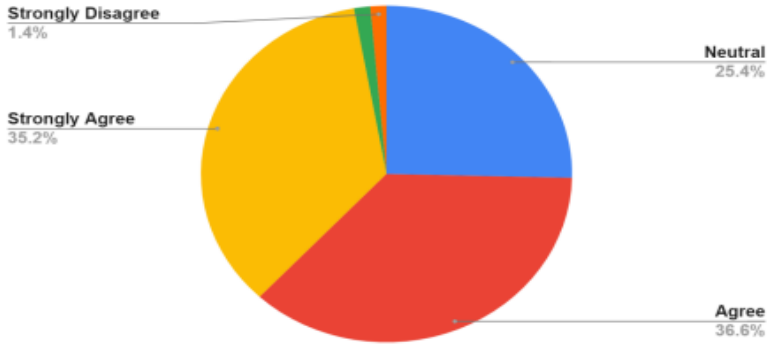
ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

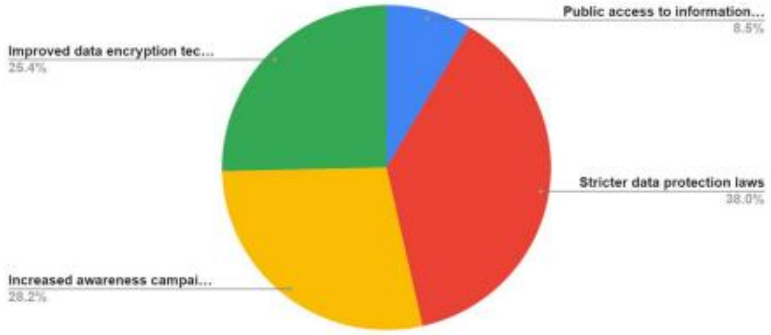
OPEN ACCESS Original Research Article

• **Do you believe stricter regulations are needed to monitor data brokers in India?**



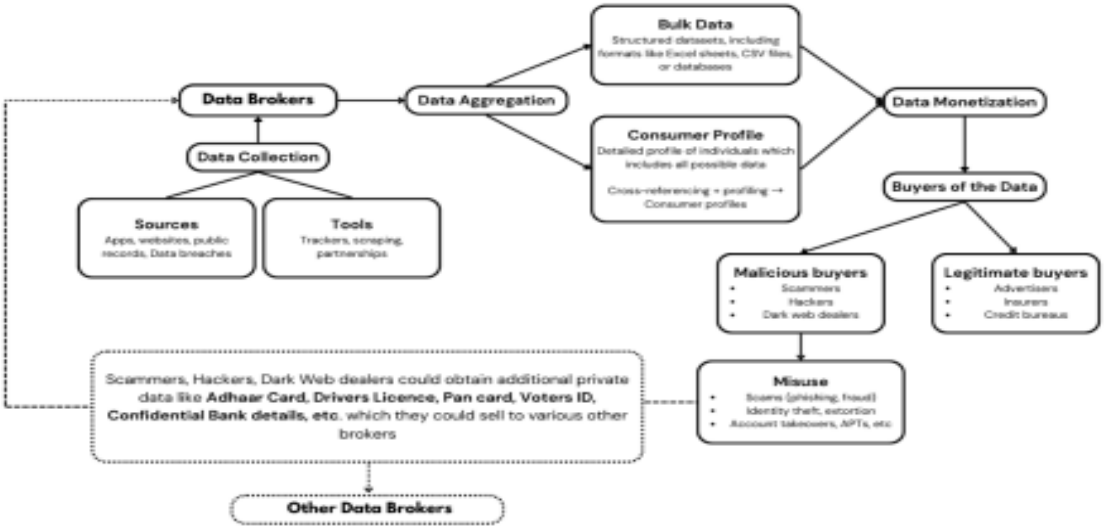
Interpretation: From the data above, 35.2% of respondents strongly agree, and 36.6% agree that stricter regulations are needed to monitor data brokers in India. 25.4% are neutral, while 1.4% disagree and 1.4% strongly disagree.

• **What measures would you suggest to reduce cybersecurity threats posed by data brokers?**



Interpretation: From the above data, 38% Favor stricter data laws, 28.2% want more awareness, 25.4% suggest better encryption, and 8.5% support public access to data broker info. The breakdown is in the table above.

Model: This is our model showing how Data Brokers operate and how can end up in the hands of cybercriminals



Interpretation: Data brokers operate in three main stages, contributing to cybersecurity threats. First, during data

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

OPEN ACCESS Original Research Article

collection, they gather information about individuals from various sources and tools, such as public records, online activity, and third-party vendors. In the second stage, data aggregation, this information is processed into monetizable formats, either as bulk datasets (e.g., Excel or CSV files) or detailed individual profiles, depending on buyers' preferences. Lastly, in the data monetization stage, brokers sell the data to legitimate buyers, such as advertisers or insurers, for purposes like targeted advertising or background checks. However, the same data can fall into the hands of malicious actors, including scammers, hackers, and dark web dealers, leading to misuse such as fraud, identity theft, or account takeovers. These criminals may also extract sensitive data, such as Aadhaar card details or confidential bank information, from victims and resell it to brokers or other malicious parties, further perpetuating the cycle.

Hypothesis Testing :

ANOVA-Test:

Null Hypothesis (H_0): There is no difference in the level of concern about personal data being collected across different age groups.

Alternative Hypothesis (H_1): There is a significant difference in the level of concern about personal data being collected across different age groups.

Anova: Single Factor

SUMMARY:

Groups Count Sum Average Variance

Age (Independent Variable) 71 140 1.971831 1.513481 Trust in organizations collecting personal data (Dependent Variable) 71 184 2.591549 1.102213

ANOVA

Source of Variation SS df MS F P-value F crit **Between Groups 13.6338 1 13.6338 10.42462 0.001549 3.908741 Within Groups 183.0986 140 1.307847**

Total 196.7324 141

P-Value is **0.001549** which is **<0.05. Therefore, reject Null Hypothesis (H0)**

Chi – Square Test:

Null Hypothesis (H_0): Data brokers do not have impact on the cybersecurity threats in India

Alternative Hypothesis (H_1): Data brokers do have impact on the cybersecurity threats in India

Do you believe data brokers contribute to cybercrimes	**Responses**
Strongly Agree	27
Agree	26
Neutral	14
Disagree	3
Strongly Disagree	1
Total	71

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

OPEN ACCESS Original Research Article

Cate-gory	Observed Frequency	Expected Frequency	Expected Proportion	Percentage Deviation	Standardized Residuals
A	27	14.2	0.19999999	+90.14%	+3.4
B	26	14.2	0.19999999	+83.1%	+3.13
C	14	14.2	0.19999999	-1.41%	-0.05
D	3	14.2	0.19999999	-78.87%	-2.97
E	1	14.2	0.19999999	-92.96%	-3.5
F				----	----
G				----	----
H				----	----

Sums:

Observed Frequencies: 71

Expected Frequencies: 71

Expected Proportions: 1.0

Reset Calculate

[Note that for df=1, the calculated value of chi-square is corrected for continuity.] [For df=1, this is the uncorrected value of chi-square.]

chi-square = 42.45

df = 4

P = <.0001

[P is non-directional]

P-Value is **<0.001. Therefore, reject Null Hypothesis (H0).**

Suggestions and Recommendations:

- **Make Data Brokers More Transparent:** Require data brokers to openly disclose how they collect, use, and sell personal data, and establish a regulatory body to monitor and enforce accountability.
- **Enhance Data Protection Regulations:** Introduce comprehensive privacy laws that require companies to implement robust security measures, like encryption, to protect personal data from breaches, and establish mandatory audits to ensure compliance.
- **Encourage nationwide campaigns:** To educate the public on data privacy, risks, and scam prevention, while incorporating data privacy programs in schools and workplaces. Encourage businesses to adopt stronger encryption and anonymization technologies, and promote collaboration between the government and private sector to improve real time threat detection systems.

Conclusion:

This research has explored the impact of data brokers on cybersecurity threats in India, shedding light on the varying concerns related to personal data collection across different demographic groups. The first hypothesis, which shows a significant difference in the level of concern about personal data collection across different age groups, was proven to be accurate. Our findings indicate that younger individuals are generally more aware and concerned about the collection of their personal data, while older age groups appear to be less informed or less concerned about the risks involved. This highlights the need for targeted education and awareness programs tailored to different demographic groups to address these concerns effectively.

The second hypothesis, which examined the impact of data brokers on cybersecurity threats in India, was also supported. The results demonstrate that data brokers play a significant role in increasing cybersecurity risks, as they aggregate and sell vast amounts of personal data that can be exploited by malicious actors. This practice contributes to the rise in identity theft, fraud, and other cybercrimes. As a result, it is crucial to implement stricter regulations and stronger safeguards to mitigate these risks and protect individuals' privacy and security.

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XIV, Special Issues– I Jan – Feb, 2025

OPEN ACCESS Original Research Article

In conclusion, this study shows the urgent need for comprehensive data protection laws, increased public awareness, and improved cybersecurity measures. Policymakers should focus on regulating the practices of data brokers, promoting transparency in data collection, and ensuring that vulnerable groups are adequately protected. Additionally, businesses and organizations must adopt advanced encryption technologies and collaborate with government agencies to enhance cybersecurity, ultimately creating a safer digital environment for all.

Bibliography / References:

- *Aaron Kamath, Purushotham Kittane, Aniruddha Majumdar, Varsha Rajesh. (2023). Privacy, Data Protection and Cyber Security in India. Mumbai: Nishith Desai Associates.*
- *Aaron Rieke, Harlan Yu, David Robinson, Joris Von Hoboken. (2016). Data Brokers In an Open Society - Upturn Report. London: Open Society Foundation.*
- *Das, S. (2018). Cyber Security and Data Protection: Challenges in the Indian Context. CLAWS Journal , 63.*
- *Germán Llorca-Abad, Lorena Cano-Orón. (2016). How Social Networks and Data Brokers trade with Private Data. Research Gate, 100.*
- *Hyeontaek Oh, Sangdon Park, Gyu Myoung Lee, Hwanjo Heo, Jun kyun Choi. (2019). Personal Data Trading Scheme for Data Brokers in IoT Data Marketplaces. IEEE Access, 11. doi:10.1109/ACCESS.2019.2904248*

Websites:

- *https://www.reuters.com/technology/cybersecurity/hacker-uses-telegram-chatbots leak-data-top-indian-insurer-star-health-2024-09-20/?utm_source=chatgp*
- *https://builtin.com/articles/top-data-broker-companies*
- *https://economictimes.indiatimes.com/tech/internet/how-data-brokers-are-selling-all your-personal-info-for-less-than-a-rupee-to-whoever-wants*
- *it/articleshow/57382192.cms?from=mdr*
- *https://www.kaspersky.com/resource-center/preemptive-safety/how-to-stop-databrokers-from-selling-your-personal-information*
- *https://www.lexology.com/library/detail.aspx?g=0 b7f02fa-6de0-41a9-99f0- 6e308de4e653*

Cite This Article:

Nair A.S., Nair D.B., Palkar S.N. & Mrs. Tiwari K.(2025). *Study on Data Brokers and their Impact on Cybersecurity Threats in India..* **In Aarhat Multidisciplinary International Education Research Journal**: Vol. XIV (Number I, pp. 23–32). ***DOI:*** ***https://doi.org/10.5281/zenodo.15250716***