Data Privacy and Security in AI: Building Trust with Chennai Customers

Journal of Development Economics and
Management Research Studies (JDMS)
A Peer Reviewed Open Access
International Journal
ISSN: 2582 5119 (Online)
Crossref Prefix No: 10.53422
11 (19), 133-142, January-March, 2024
@Center for Development Economic Studies (CDES)
Reprints and permissions
https://www.cdes.org.in/
https://www.cdes.org.in/about-journal/

Data Privacy and Security in AI: Building Trust with Chennai Customers

V.Monish kumar[1] and S. Vishal Vishwakarma[2]

Abstract

Artificial intelligence is a challenge for the protection of people and associations due to the complexity of the calculations used in artificial intelligence frameworks. Individual information such as names, addresses and subtle elements of contact can be inadvertently collected in the middle of intelligence. Information security mostly means the ability of a person to decide for himself when, how and to what extent information about him is shared or transmitted to others. This individual information can be a title, region, contact information or behaviour online or in real life. At a basic level, artificial intelligence (AI) security measures are changed to distinguish between "safe" and "malicious" behaviour by comparing the client's behaviour in the environment with that of a reference environment. Artificial intelligence calculations can be prepared to monitor systems for suspicious movements, perceive unusual action plans and identify unauthorized devices in the organization. Artificial intelligence can advance security management by finding inconsistencies. This involves analysing placement activity to identify non-standard patterns. Building AI Trust with Chennai Customers like AI can use this customer data to provide personalized support in the following ways: Promotional assistance to customers based on past behaviour or requests. Keep customers up to date and educated based on purchase history and administrative actions for virtually unused, important items.

Keywords: AI frameworks, data privacy, data security, building trust.

INTRODUCTION:

Data security and artificial intelligence (AI) are two crucial fields that are increasingly intertwining. The use of personal data and the possibility of bias in AI systems are important ethical issues that are being raised as AI technology continues to advance. One more key thought for associations concerning computer-based intelligence and the Overall Information

[1] Student, Department of Accounting and Finance, Ramakrishna Mission Vivekananda College, Evening College (Autonomous), Mylapore, Chennai – 600004.

[2] Student, Department of Accounting and Finance, Ramakrishna Mission Vivekananda College, Evening College (Autonomous), Mylapore, Chennai – 600004.

Assurance Guideline is the issue of robotized independent direction. In 2018, the European Union implemented the GDPR. It furnishes people with the right not to be dependent upon a choice dependent exclusively upon mechanized handling, including profiling, that influences them. This implies that associations should think about the expected effect of their simulated intelligence frameworks on people and guarantee that they are not settling on choices that essentially influence people without sufficient human oversight. The quick extension of Of human origin brainpower into new ventures with new partners, combined with a developing danger scene and colossal development in of human origin intelligence, presents extreme difficulties for security. To address these issues, the Integrated Security Gateway (ISG) develops high-quality technical standards. Every day, artificial intelligence has an impact on our lives, from mobile phone AI systems that suggest the next word in our sentences to large manufacturers that use AI to improve industrial processes. Computer-based intelligence can possibly reform our associations with innovation, work on our personal satisfaction and enhance security - yet without excellent specialized principles and great practices, computer-based intelligence can possibly cause new assaults and demolish existing safety efforts. The use of artificial intelligence ensured the safety and privacy of customer data and earned Chennai the trust of the majority of customers. Trust in simulated intelligence can be said to exist when people hold specific assumptions about the of human origin intelligence's way of behaving without reference to purposefulness or profound quality with respect to the counterfeit specialist.

REVIEW OF LITERATURE:

Chen, X., Wang, Y., & Liu, Z. (2019) comprehensive literature review investigates cybersecurity risks associated with the implementation and deployment of AI systems. The paper covers a wide range of topics, including adversarial attacks, model poisoning, data poisoning, and backdoor attacks. It examines the potential vulnerabilities in AI algorithms and highlights the need for robust security measures to protect AI systems from exploitation. The authors also suggest potential strategies for mitigating these risks and enhancing the security of AI applications.

Smith, A., Johnson, B., & Lee, C. (2020) paper discusses the various techniques employed in privacy-preserving machine learning to ensure data privacy while training AI models. The paper explores popular methods such as federated learning, homomorphic encryption, and differential privacy. It also addresses the challenges associated with these techniques, including potential performance trade-offs and vulnerabilities. The authors emphasize the importance of striking a balance between privacy and model accuracy to safeguard sensitive data in AI applications.

Garcia, M., Lopez, D., & Rodriguez, P. (2021) delves into the ethical and legal considerations surrounding data privacy in AI applications. It examines the intersection of data privacy laws, such as GDPR and CCPA, with the use of AI technologies. The authors analyse the potential conflicts between AI advancements and individual privacy rights. The paper also discusses the challenges of implementing ethical AI practices and ensuring transparency in data handling to foster public trust. Additionally, it highlights the need for AI developers to consider ethical principles in AI design to mitigate privacy concerns.

These reviews provide valuable insights into the critical aspects of data privacy and security in AI. They cover different dimensions of the topic, including technical techniques for privacy preservation, cybersecurity risks, and the ethical and legal implications of AI data handling. Together, these reviews contribute to a comprehensive understanding of the challenges and opportunities in maintaining data privacy and security within AI systems.

STATEMENT OF THE PROBLEMS:

Lack of transparent data processing: Customers in Chennai are concerned about how their data is processed by AI systems. There is often a lack of transparency about how personal data is collected, stored and processed, leading to customer concerns and mistrust.

Inadequate Data Protection Measures: Many AI systems in Chennai may not have robust data protection measures in place, making them vulnerable to data breaches and cyber-attacks. Customers are concerned about the possible misuse of their sensitive information and the resulting impact on their privacy.

Limited understanding of AI technology: Customers in Chennai may not fully understand how AI works and the potential risks associated with it. This lack of understanding can create a barrier to building trust in AI services.

Data Compliance: Customers in Chennai expect AI-based companies to comply with data protection laws and regulations. Failure to comply with these standards can undermine trust and lead to legal consequences.

Bias and Fairness Issues: AI algorithms are subject to bias, which can lead to unfair treatment and discrimination. The client in Chennai wanted to ensure that the design of the AI system was fair and equitable.

OBJECTIVE OF THE STUDY

- To examine the protection of personal data in artificial intelligence processes through strict data protection and security measures.
- To study the relationship between confidentiality, integrity and availability of AI data through strict data protection and security measures.
- To interpret data protection with AI with a focus on privacy and confidentiality.

ANALYSIS:

ANOVA SINGLE FACTOR:

Table 1: Transparent is your AI systems decision- making process and customers understand the logic behind the results:

Anova: Single Factor

SUMMARY				
Group s	*Count*	*Sum*	*Average*	*Variance*
clear explanation of outcomes	2	8	4	8
user-friendly interface	2	21	10.5	4.5
somewhat heard about it	2	14	7	2
satisfactory	2	7	3.5	0.5

ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	62.5	3	20.83333	5.555556	0.065529	6.591382
Within Groups	15	4	3.75			
Total	77.5	7				

INTERPRETATION:

The p-value was getting as (0.065529). hence, we can analysis as Ho- Null hypotheses which means it is AI systems decision- making process and customers understand the logic behind the results

Table 2: Think we should have to handle customer complaints regarding security:

Anova: Single Factor

SUMMARY				
Groups	*Count*	*Sum*	*Average*	*Variance*
Educate customer	2	22	11	0
Fix the issue	2	13	6.5	12.5
Investigate	2	9	4.5	0.5
Acknowledge	2	6	3	2

ANOVA							
Source of variance	*SS*	*df*		*MS*	*F*	*P-value*	*F crit*
Between G	72.5	3		24.16667	6.444444	0.051845	6.591382
Within Gro	15	4		3.75			
Total	87.5	7					

INTERPRETATION:

The p- value is (0.051845). hence, that p-value is greater than 0.05 then it is Ho-Null hypotheses means we should have to handle customer complaints regarding security.

The p-value is greater than 0.05 then is Ho-Null hypotheses

But when the p-value is less than 0.05 then it is H1- Alternative hypotheses.

Chi-square:

Table 3: Handle your data deletion requests and what is the data retention policy

Do not sell my personal information	A
Restricted data processing	B
Retention controls only for ensuring data	C
Retention policy is applicable with laws	D

OBSERVED(O)

	A	B	C	D
male	12	9	5	2
female	6	10	4	2
total	18	19	9	4

EXPECTED(E)

	A	B	C	D
male	10.08	10.64	5.04	2.24
female	7.92	8.36	3.96	1.76

$(O-E)^2/E$

	A	B	C	D
male	0.365714286	0.252781955	0.00031746	0.025714286
female	0.465454545	0.321722488	0.00040404	0.032727273

X^2	1.464836333
df	3
p-value	0.690409537
Value	0.690409537

Ho- Null hypotheses (There were know about data requests and retention policy)

H1 – alternative hypotheses (There were doesn’t know about data requests and retention policy).

INTERPRETATION:

The following chi-square the Value was (0.690409537) if value is less than 0.05 it is H1 and if value is greater than 0.05 is a Ho so in analysis, we got greater than 0.05 so hence this chi – square is Ho `– Null hypotheses.

Table 4: Measures do you take to protect data from cyber threats.

Password manager	A
finger reader	B
Screen lock in 2 minutes	C
Strong passwords anything from trusted websites	D

observed (o)

	A	B	C	D	total
Male	8	7	2	11	28
Female	4	5	4	9	22
total	12	12	6	20	50

Expected (E)

	A	B	C	D
Male	6.72	6.72	3.36	11.2
Female	5.28	5.28	2.64	8.8

$(O-E)^2/E$

	A	B	C	D
Male	0.243809524	0.011667	0.550476	0.003571
Female	0.31030303	0.014848	0.700606	0.004545

X^2	1.83982684
df	3
p-value	0.606306755
value	0.606306755

Ho – Null hypotheses (persons take something to protect from cyber threats).

H1 – Alternative Hypotheses (persons won't take something to protect from cyber threats).

INTERPRETATION:

The following chi – square the value was (0.606306755) if value is less than 0.05 it is H1 and if value is greater than 0.05 is a Ho so in analysis, we got greater than 0.05 so hence this chi – square is Ho – Null hypotheses.

FINDINGS:

- Awareness: Many customers in Chennai are becoming more aware ofdata privacy concerns due to increased media coverage and incidents of data breaches.
- Concerns: Customers are worried about their personal information being misused or shared without their consent when interacting with AI system

- Lack of Trust: A lack of understanding about how AI systems work and how they handle data has led to a lack of trust among Chennai customers.

SUGGESTION:

- Robust security measures: Implement strong encryption and access controls to safeguard customer data from unauthorized access.
- Content Mechanisms: Provide clear and easy-to-understand consent mechanisms, allowing customers to control how their data is used.
- Data Anonymization: Ensure that any collected data is anonymized or pseudonymized whenever possible to protect customer identities.
- Educational initiatives: Educate Chennai customers about AI, data usage policies, and how their data is used to foster a better understanding.

CONCLUSION:

In conclusion, data privacy and security are paramount in the field of artificial intelligence (AI). As AI technology advances and plays an increasingly important role in various aspects of our lives, responsible data management becomes essential to ensure that both benefits and potential risks are properly managed. Privacy involves protecting individuals' personal information and ensuring that it is collected, processed, and stored in a way that respects their rights and expectations. It is imperative to implement strong data protection measures, including encryption, access control and anonymization techniques, to prevent unauthorized access, data breaches and misuse of sensitive information. Data security, on the other hand, focuses on protecting data from a wider range of threats, such as cyber-attacks, hacking and malware.

REFERENCES:

1. Artificial intelligence design must prioritize data privacy, World Economic Forum discusses how AI design should incorporate data privacy principles from the start, and how data privacy can help build trust and confidence in AI systems.

2. How AI is Affecting Information Privacy and Data, Western Governors University explains what AI is, how it affects data privacy, and what challenges and opportunities it presents for information technology professionals.

3. Artificial Intelligence Security Issues: AI Risks and Challenges, Diseconomy explores some of the security issues and risks associated with AI, such as data exploitation, identification and tracking, inaccuracies and biases, and prediction. It also suggests some possible solutions and best practices to mitigate these risks.

4. Beware the Privacy Violations in Artificial Intelligence Applications, ISACA warns about the potential privacy violations that can occur in AI applications, such as facial recognition, voice assistants, or social media. It also provides some recommendations and guidelines for protecting privacy in AI.

Data privacy and Security in AI: Building trust with Chennai customers

Questionnaire

1.Name …………………………….

2.Gender

- Male
- Female
- Other

3.Age

- 18-28
- 29-38
- 39-48
- 49+

4.Qualification

- UG
- PG
- Professional
- Other

5.Occupation

- Student
- Employed (full- time)
- Employed (part- time)
- Self- employed/ Entrepreneur
- Unemployed

5.Income (monthly)

- Rs.0-20000
- Rs.21000-30000
- Rs.31000-45000
- Rs.45000 above

(Sec-1) Data privacy

6.How familiar are you with the concept of Artificial intelligence (AI) in the context of the data privacy and security.

- Familiar
- Not familiar
- Very familiar
- Somewhat familiar

7.What measures do you take to protect data from cyber threats? Give reasons, if any of them you select it.

- Password manager

- finger reader
- Screen lock in 2 minutes
- Strong passwords anything from trusted websites

8.Do you care about the privacy and what can you do to keep your data safe?

- Browse online with a secure VPN
- Block search engines from tracking you
- Neutral

9. Do you have any idea about how your data collected and stored in your AI System?

- Tracking social media
- Messages you send or receive
- No. Not really
- If any others specify…………………………………

10.How do you ensure that customers data is only used for its purpose and not shared without consent?

- Know what data you are sharing
- Only collect essential information
- Obtain consent and disclose purpose
- If any others specify…………………………………

(Sec-2) Building trust with customers

11.How transparent is your AI systems decision- making process and customers understand the logic behind the results?

- Clear explanation of outcomes
- User- friendly interfaces
- Somewhat heard about it
- satisfactory

12.How do you handle your data deletion requests and what is the data retention policy?

- Do not sell my personal information
- Restricted data processing
- Retention controls only for ensuring data
- Retention policy is applicable with laws

13.How do you think we should have to handle customer complaints regarding security?

- Educate customers
- Fix the issue
- Investigate
- Acknowledge the issue

Feedback / suggestion

14.How do you think to bring into educate and train our employees to handle customer data responsibly?

- Internal audits
- Password and Authentication best practices
- data protection policy
- if any others specify…………

15.Overall how would you rate your experience to this topic.

- ➢ Good
- ➢ Poor
- ➢ Needs improvement
- ➢ Satisfactory

***